تعلم بدون تعقيد©

أساليب الأمن والحماية في ويندوز إكس بى



المركز الرئيسى : 11 شارع د/محمد رأفت – محطة الرمل – الإسكندرية
تليفون وفاكس : 4838326 (03)(2+)
موبايل : 0101634294 (2+) - 0123357844 (2+)
Email: info@egyptbooks.net
URL: www.egyptbooks.net

محمد عبد الكريم

رقم الإيداع

25139 / 2007

إهداء

روى عن رسول الله صلى الله عليه وسلم أنه قال : من لم يشكر الناس لم يشكر الله ، وإنى أشكر الله سبحانه وتعالى ها هنا وأرد الحق لمستحقيه وأهدى كتابى هذا لكل أساتذتى ومن تعلمت على أيديهم وجعلهم الله سبباً فيما صيرت إليه ولكل إنسان لم يبخل علىّ بوقته أو بمعلومة أو بنصيحة .. فهؤلاء جميعاً أضاءوا لى الطريق ولهم على الكثير من الفضل من بعد الله سبحانه وتعالى وإليهم جميعاً أهدى كتابى هذا كلمة شكر وإمتنان أرجو أن تصل إليهم .

إلى أبى وأمى وعائلتى وأصحاب الحقوق على أهدى هذا الكتاب .

المقدمة

الحمد لله كما ينبغى لجلال وجهه وعظيم سلطانه وصلى اللهم على سيدنا محمد وعلى آل سيدنا محمد وسلم تسليماً كثيراً ، أما بعد ..

أصبح الإحساس بالأمن والطمأنينة الأن من أهم الأهداف والأمانى التى يسعى إليها أى شخص يحيى فوق ظهر هذا الكوكب .. وينطبق هذا الهدف أيضاً على عالم أخر أقل حجماً ولا ينفصل بحال من الأحوال عن هذا العالم الكبير ألا وهو الكمبيوتر فلم يعد الكمبيوتر الأن مجرد جهاز ترفيهى أو من كماليات الحياة بل أصبح أحد أساسيات الحياة العصرية بل إن شئت فقل أحد أساسيات حياتنا الشخصية ولم لا وقد أصبح كل ما يدور من حولنا فى شتى مجالات الحياة مرتبط به إرتباطاً وثيقاً .. وبالنسبة لنا فقد أصبح كالصديق أو كاتم الأسرار أو الخزينة التى تحوى بداخلها أدق التفاصيل المتعلقة بالجوانب المختلفة لحياتنا وإهتماماتنا من عمل أو تعليم أو ... أو ...

وبالتالى فقد أصبحت أى محاولة إعتداء عليه أو إختراق له هى فى الحقيقة إعتداء على حرياتنا وإقتحام لحياتنا الخاصة بكل جوانبها وإنتهاك لأدق خصوصياتنا. ولذلك سنقوم سوياً من خلال صفحات هذا الكتاب بالتعرف على الأساليب التى يمكن أن يتبعها أو يلجأ إليها أحد (المتطفلين) من أجل التسلل إلى هذا الجزء من حياتنا وسنتعرف أيضاً على تلك الثغرات التى يقومون بإستغلالها داخل نظام التشغيل وينوز

اكس بى والتى يرجع الكثير من أسباب وجودها إلى أخطاء وتهاون منا وسنتعلم كيف لنا أن نقوم بسد هذه الثغرات وتلافى تلك الأخطاء بل سنتعرض لما يمكن أن يكون أكبر من ذلك والتعامل معه من أجل أن نحافظ خصوصياتنا أمنة بعيداً عن أيدى هؤلاء العابثين ... وقد راعيت أثناء إعدادى لهذا الكتاب أن لا يكون موجه فقط لأصحاب الخبرة أوالمحترفين ولكن أيضاً المبتدئين لأننا جميعا نشترك فى هدف واحد وجميعنا نسعى إلى أبسط حقوقنا فى الشعور بحياة أمنة بعيدة عن هؤلاء الغرباء والمتلصصين ولذلك ستجد أن الكتاب يقوم بشرح المعلومة بأكثر من طريقة سيجد من بينها المبتدىء ما يناسبه وكذلك سيجد المحترف ما يبحث عنه ويرضى غروره لكى نصل فى النهاية إلى أن الجميع أصبح يملك من الأدوات ولديه من الحيل والأساليب ما يستطيع به التحدى والتصدى إلى أى شخص يحاول إقتحام أو إختراق الويندوز بطريقة أو بأخرى ... وأرجو الله سبحانه وتعالى أن يجعله خالصاً لوجه الكريم ...

قال رسول الله صلى الله عليه وسلم

من أصبح منكم آمناً في سربه، معافىً في جسده، عنده قوت يومه فكأنما حيزت له الدنيا بحذافيرها .

صدق رسول الله صلى الله عليه وسلم



الفصل الأول

إغلاق الأبواب

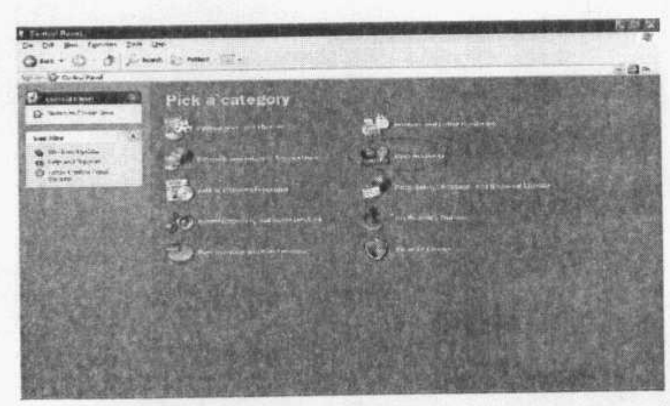
إغلاق الأبواب

هذا الفصل هو نقطة الإنطلاق التى سنبدأ منها رحلتنا فى الدفاع عن أنفسنا ضد كل من تسول له نفسه التطفل أو التطلع إلى الحاسب الخاص بنا وأول ما نبدأ به مشوارنا أو معركتنا هذه هو إنشاء كلمة مرور للحاسب وبالطبع يوجد الكثير ممن يستطيعوا القيام بذلك بسهولة ولكن للأسف أنه يوجد الكثير أيضاً ممن يجهلون طريقة القيام بذلك مما جعلنى أبدأ تلك البداية (من نقطة الصفر) كما أنك إذا أردت أن تقوم بإغلاق الشبابيك فلا بد أولاً أن تكون الأبواب مغلقة !!! وأعتقد أن الجميع يعرف هذا ولكن هنا سنراجع سوياً إغلاق هذه الأبواب من البداية وذلك لوجود الكثير ممن يجهلون طرق إغلاق تلك الأبواب وهذا فضلاً عن من يجهلون وجودها أصلاً !!! وأعتقد أن الأمانة تحتم علينا أن لا نترك هؤلاء (الأبرياء) ضحايا وفريسة سهلة فى عالم يسيطر عليه الأشرار ..

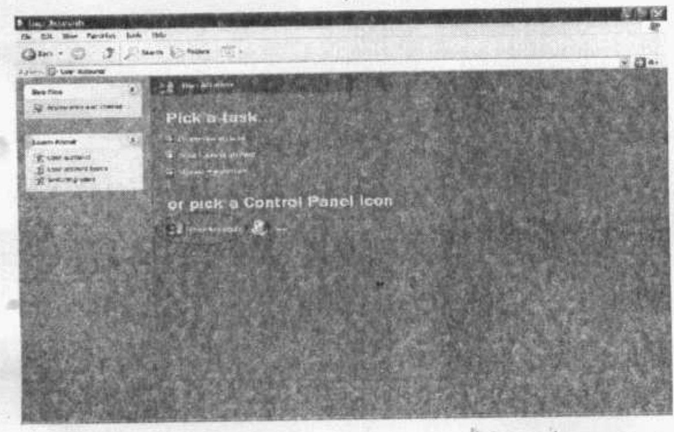
سبب أخر يجعلنا نبدأ تلك البداية أنه ربما تكون قد غابت عنك أحد النقاط أو نسيت إغلاق أحد هذه الأبواب وهذا من الأخطاء التى يتمناها اللصوص أيضا ويعتمدون عليها فى إختراق اجهزتنا وإقتحام حياتنا بدون سابق إنذار !.. كما أن هذه الخطوات لن تضرنا فى شئ ولكن بدونها قد نخسر الكثير ...

إنشاء كلمة سر :

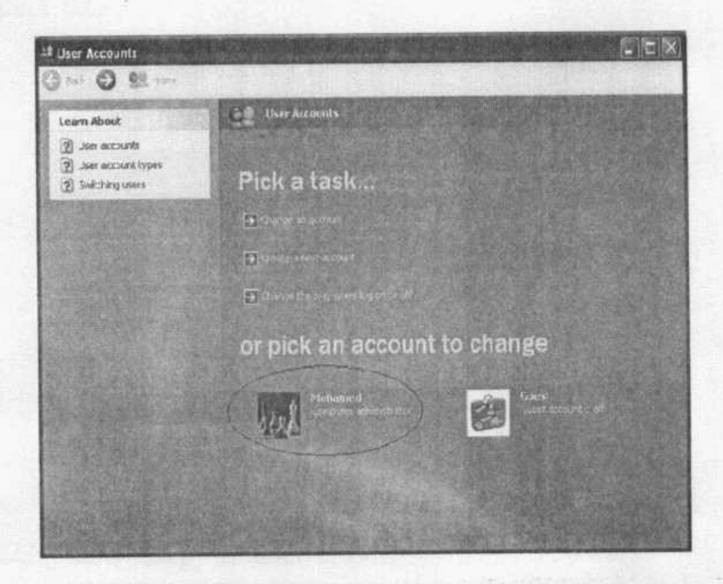
من قائمة start نقوم بإختيـــار Control Panel لتظهـــر لنـــا النافذة التالية:



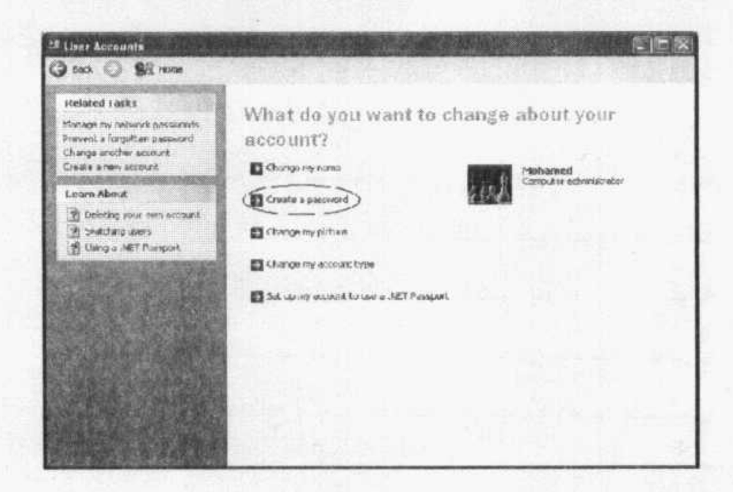
من النافذة السابقة نقوم بالضغط على User Accounts المـــشار إليـــه بالشكل السابق لتظهر لنا النافذة التالية :



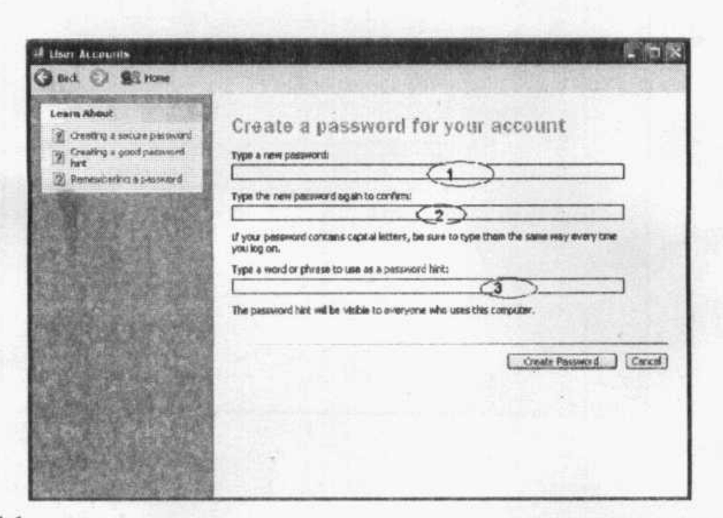
من النافذة السابقة نقوم أيضاً بالضغط على User Accounts المشار إليه لتظهر لنا النافذة التالية :



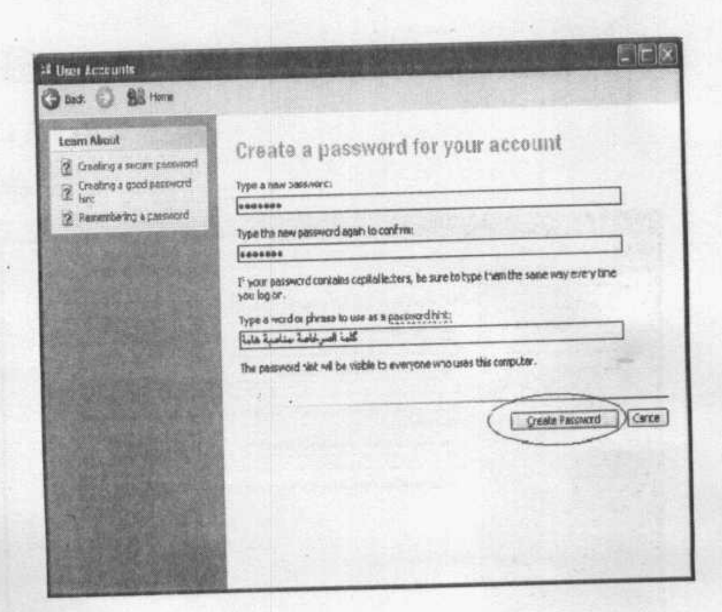
من النافذة السابقة يظهر حساب Guest أو الضيف وهذا سنتعامل معه فيما بعد .. ولكن ما يهمنا هنا هو الحساب الخاص بالمستخدم المشار إليه بالشكل السابق وبالطبع يمكن أن يحتوى الجهاز على أكثر مستخدم والأن نقوم بالضغط على اسم المستخدم المراد إنشاء كلمة مرور له وهو فى حالتنا هنا بالإسم Mohamed كما هو موضح لتظهر لنا النافذة التالية :



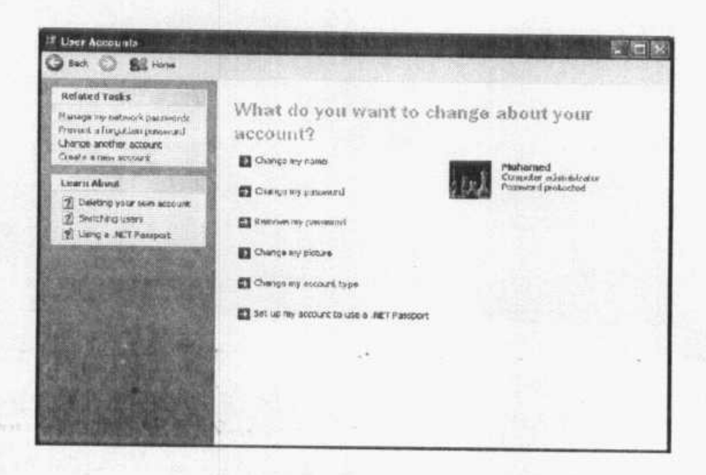
من النافذة السابقة نقوم بالضغط على Create a password لتظهر لنا النافذة التالية :



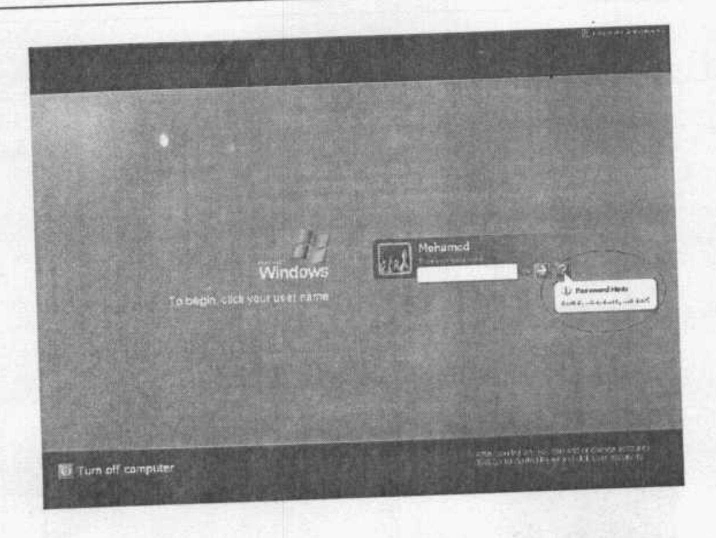
1. قم هنا بكتابة كلمة السر التى تريدها .
2. قم هنا بإعادة كتابة كلمة السر .
3. قم هنا بكتابة كلمة تذكرك بكلمة المرور .. ويجب التنبيه أن ما تكتبه هنا يمكنك الإستغناء عنه وعدم كتابته فهو مجرد ملاحظة فقط وليس كلمة السر نفسها لأنه وجد الكثير يقومون هنا بكتابة كلمة السر وهم بذلك يكونون مثل من أغلق باب المنزل بالمفتاح وترك المفتاح بالباب !!! لتصبح النافذة كما بالشكل التالى :



بعد أن تنتهى قم بالضغط على الزر Create Password ليتم إنشاء كلمة السر وتظهر لك النافذة التالية .



قم بإغلاق النافذة السابقة لتكون بذلك قد إنتهيت من إنشاء كلمة السر وعند دخولك للجهاز فى المرة القادمة ستجد هذه الشاشة فى إنتظارك تطالبك بإدخال كلمة المرور لتستطيع الدخول للويندوز .

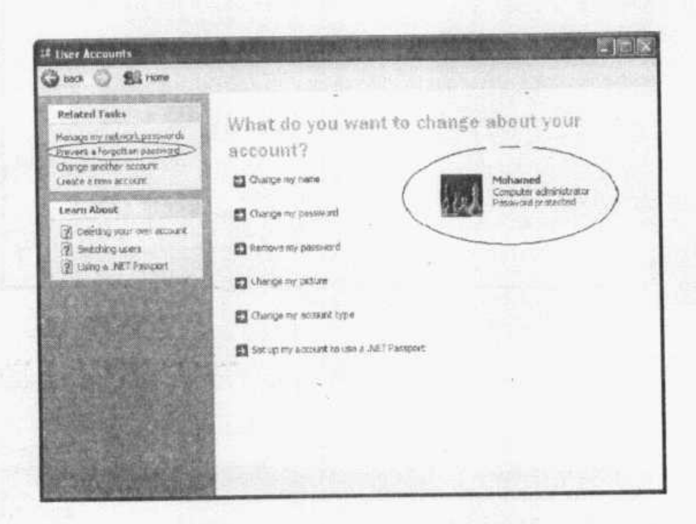


لاحظ أنه فى حالة نسيانك كلمة المرور يمكنك أن تقوم بالضغط على أيكونة علامة الإستفهام (؟) ليظهر لك التلميح الذى أدخلته سابقاً لتذكيرك بكلمة السر كما موضح بالشكل السابق .

حل أخر لنسيان كلمة المرور :

إذا كنت تخشى من نسيان كلمة المرور ولا تطمئن إلى تذكرها فيمكنك أن تقوم بالإحتفاظ بها على قرص مرن والإحتفاظ إلى حين إحتياجه وسيسمح لك هذا القرص فيما بعد إذا نسيت كلمة أن تقوم بتغيير كلمة المرور هذه بكلمة أخرى جديدة وذلك بإتباع الخطوات التالية .

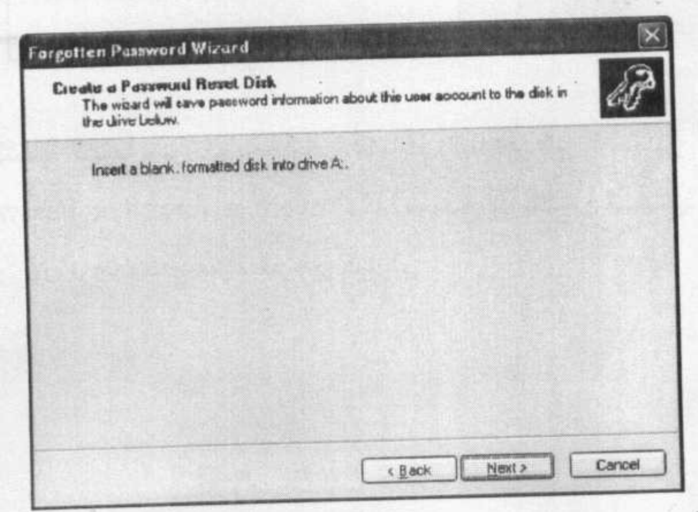
قم بالذهاب إلى نافذة Control Panel ومنها إلى user Accounts ثم إلى Accounts أو الحساب الذى تريده وهو فى حالتنا هنا بالإسم Mohamed كما بالشكل التالى :



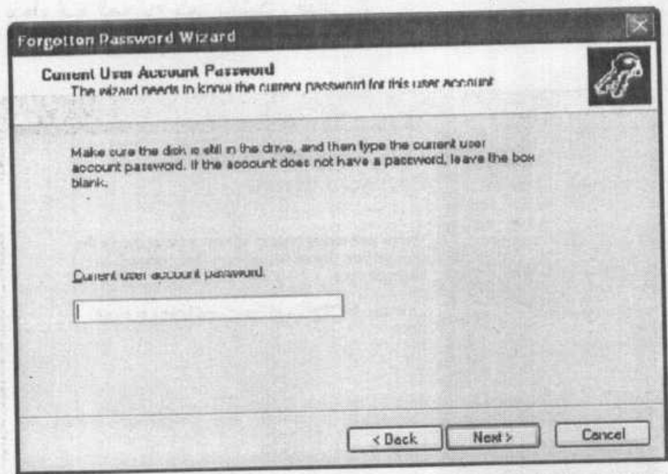
من الشاشة السابقة ومن الجهة اليسرى منها قم بالضغط على الإختيار Prevent a forgotten Password كما موضح لك بالشكل السابق ليظهر أول نوافذ معالج إنشاء القرص كما يلى :



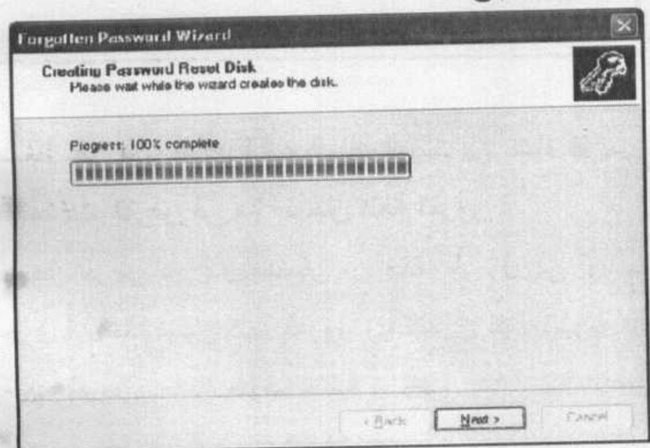
قم بالضغط فوق الزر Next لتظهر لك النافذة التالية :



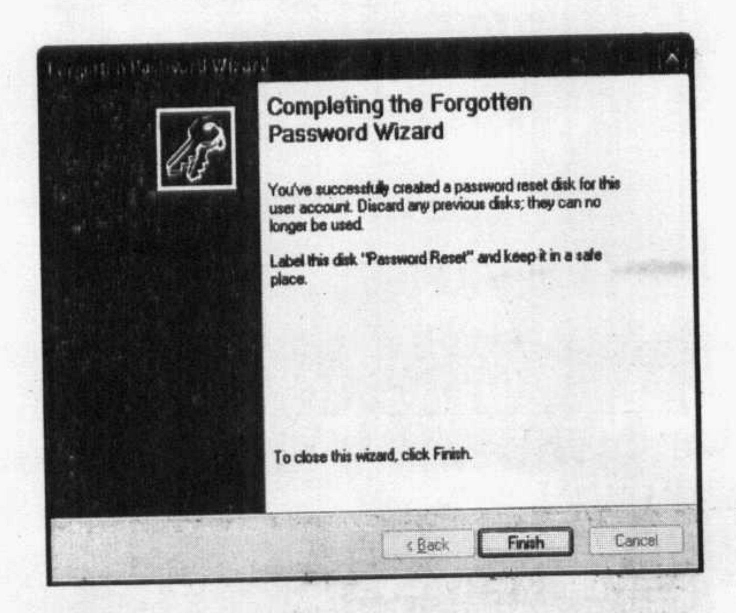
قم الأن بوضع قرص مرن داخل محرك الأقراص ثـــم اضـــغط Next لتنتقل إلى النافذة التالية :



قم بإدخال كلمة المرور الخاصة بالمستخدم ثم اضغط الزر Next يبـــدأ إنشاء القرص كما يلى :



بعد أن ينتهى المعالج من عمله قم بالضغط على الزر Next لتنتقل إلى أخر خطوات المعالج كما بالشكل التالى :

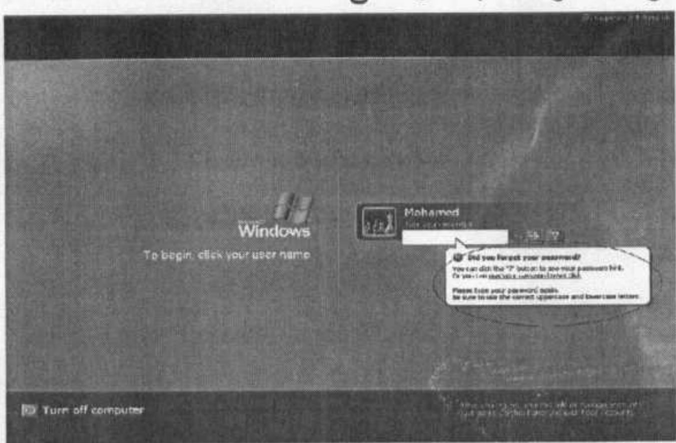


قم بالضغط على الزر Finish لتكون بذلك إنتهيت من إنشاء القرص .

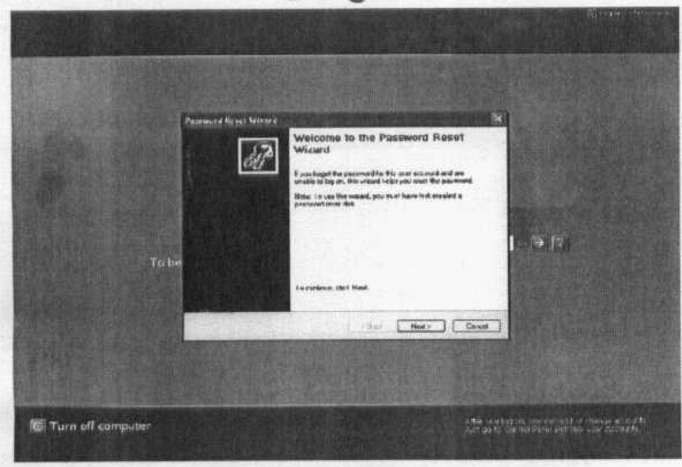
طريقة إستخدام القرص فى حالة نسيان كلمة المرور :

هذا القرص هو الذى ستتمكن من خلاله الدخول إلى الويندوز مرة أخرى فى حالة نسيان كلمة المرور ويمكنك أن تقوم بتجربة فاعلية وأهمية هذا القرص كما بالخطوات التالية .

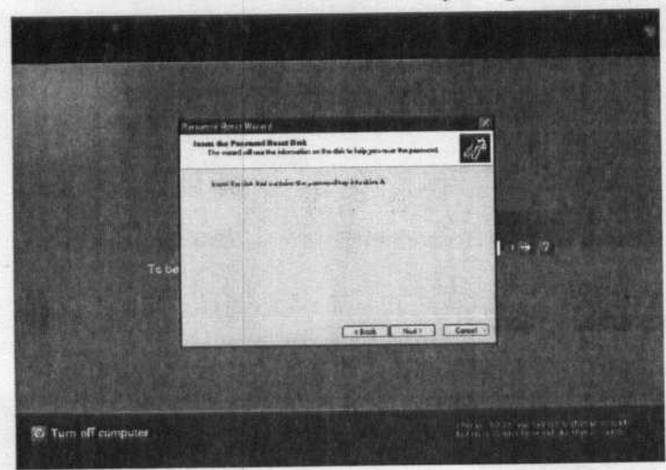
فى شاشة الدخول إلى الويندوز قم بإدخال كلمة سر غير صحيحة لتظهر لك الرسالة الموضحة بالشكل التالى :



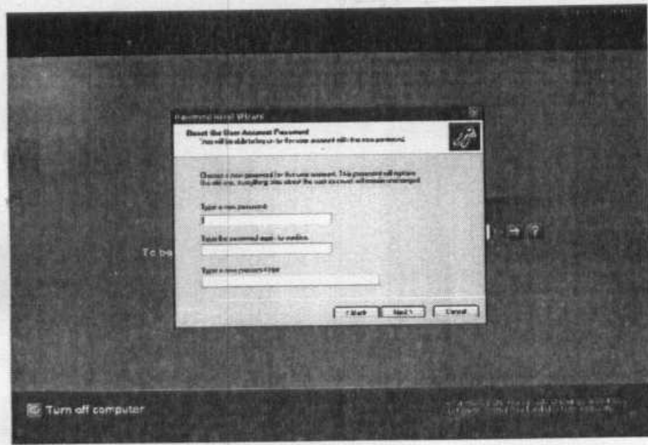
من الرسالة السابقة قم بالضغط على الإختيـــار use your password reset disk ليظهر لك نافذة المعالج التالى:



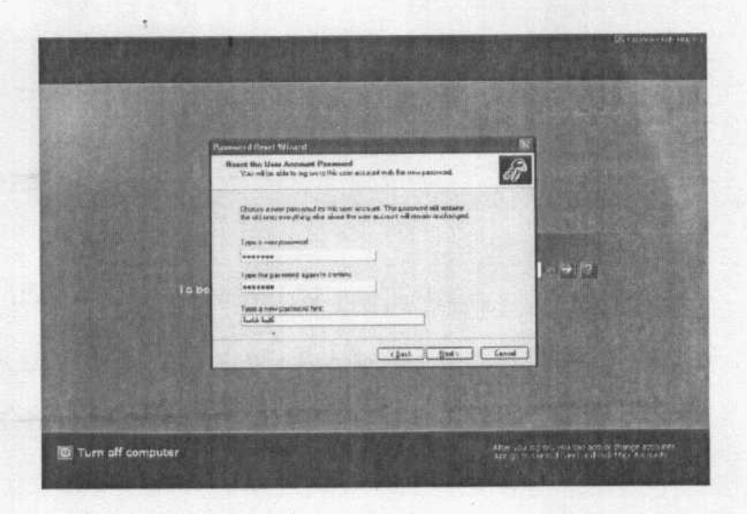
النافذة السابقة ترحب بك وتخبرك بوظيفة المعالج .. قم بالضغط علـــى Next لتنتقل للخطوة التالية :



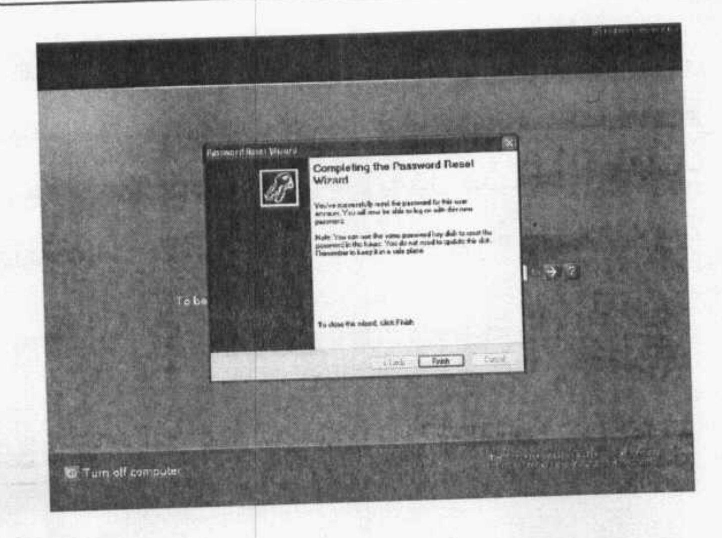
قم بإدخال القرص داخل محرك الأقراص ثم اضغط الزر Next لتنتقل إلى الخطوة التى تليها .



من النافذة السابقة ومن خلال مربع النص الأول قم بإدخال كلمة المرور الجديدة ثم أعد كتابة كلمة المرور مرة أخرى فى مربع الـــنص الثـــانى وفى مربع النص الثالث يمكنك أن تقوم بإدخال كلمـــة لتـــذكرك بكلمـــة المرور وبعد أن تنتهى ستصبح النافذة كما بالشكل التالى .



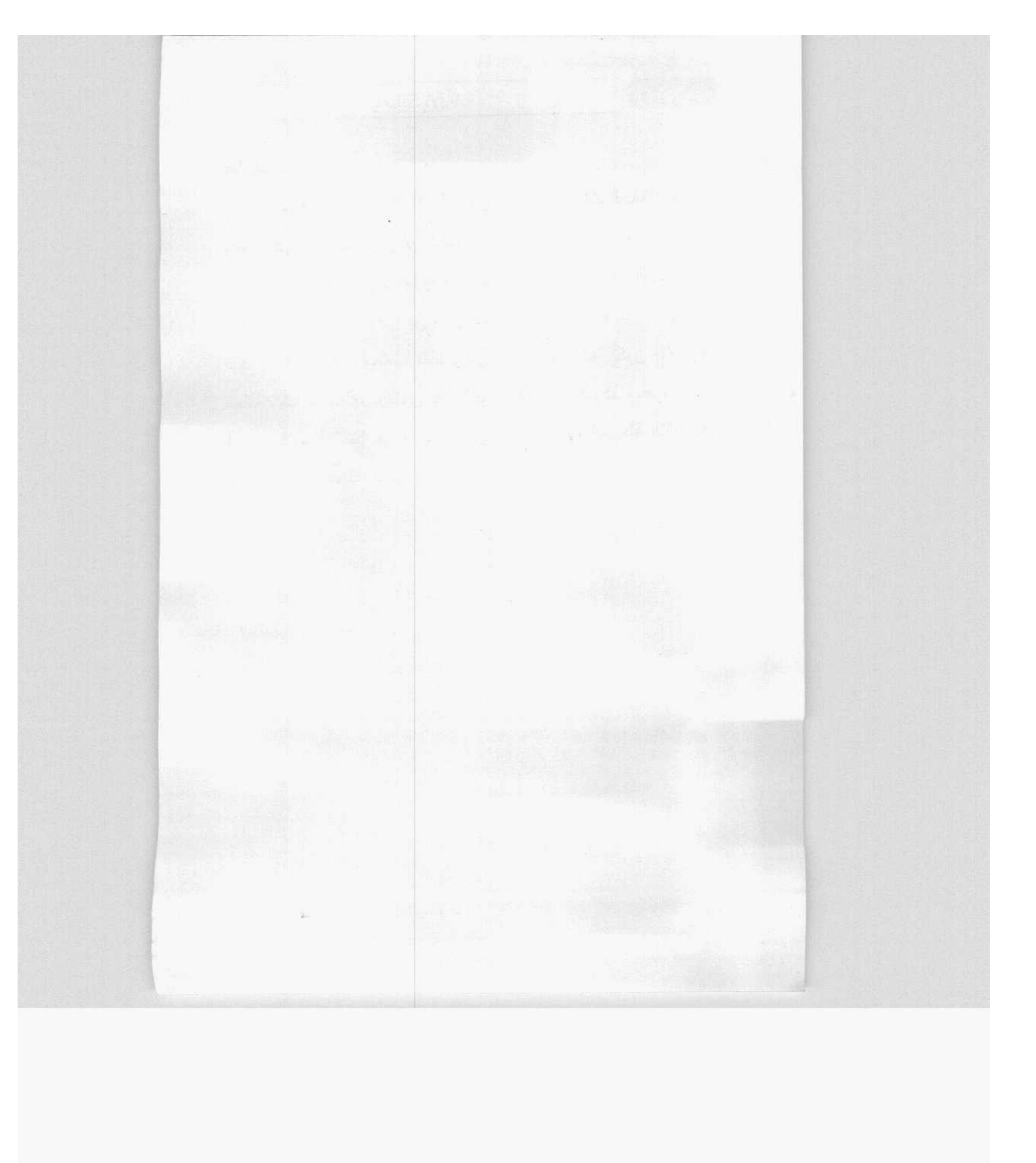
قم الأن بالضغط على زر Next لتنتقل إلى الخطوة الأخيرة كما بالشكل التالى .



قم بالضغط فوق زر Finish لتكون بذلك انتهيت من تغيير كلمة المرور ثم قم بعد ذلك بإدخال كلمة المرور الجديدة بالطريقة العادية واضغط Enter لتصبح داخل الويندوز .

أما بعد ..

ما قمنا به فى هذا الفصل ومن خلال الخطوات السابقة هو مـــا يعلمه أكثر المستخدمين وهو كذلك من أساسيات الحماية ومجرد بدايـــة وليس هذا هو كل شيء كما يعتقد الكثير ويظنون أنهم بعد القيام بمثـــل تلك الخطوات قد أصبحوا فى مأمن وبعيداً عن أيدى العابثين .. ولكـــن ذلك لا يكفى لتكون مطمئناً فاللصوص يعلمون ان دائما تكون الأبـــواب مغلقة وهذا مايجعلهم يبحثون عن الأبواب الخلفية والنوافذ ويقفزون فوق الأسوار! وهذا أيضاً هو ما سنتعرض له ونفعله فى المرحلة التالية لكى نقوم بتأمينه وإغلاقه أمامهم .



الفصل الثاني

الأبواب الخلفية

الأبواب الخلفية

سنتناول فى هذا الفصل الأبواب الخلفية التى يمكن أن تشكل لنا تهديداً أو يمكن أن يتم إستغلالها فى الدخول إلى الويندوز وإختراقه خاصةً أنها لا تتطلب مجهوداً أو خبرة كبيرة وأول وأهم ما يتم إستغلاله من تلك الأبواب الخلفية هو الحساب الخاص بالمدير أو Administrator وتعود الخطورة هنا إلى أن هذا الحساب تكون له جميع الصلاحيات وبدون أى قيود بل العكس يكون صحيحاً فمدير الكمبيوتر هذا يمكنه أن يقوم بوضع أى قيود على أى من مستخدمى الجهاز أو حذفهم نهائياً .. والبداية تعود إلى وقت إعداد الويندوز فأثناء ذلك تظهر لك أحدى النوافذ لتطالبك بإدخال كلمة المرور الخاصة بمدير الجهاز (Administrator) ومن الأخطاء الشائعة أن الكثير يتجاهل هذه النافذة ويتخطاها بعدم مبالاة يحسدون عليها ! فإن كنت تقوم بإعداد الويندوز بنفسك فأنت بالطبع تعرف هذه النافذة وقابلتها كثيراً وتعرف ما كنت تفعله حيالها .. وإن كنت لا تقوم أنت بإعداد الويندوز الخاص بك فعليك الأن التأكد من سد تلك الثغرة وحماية نفسك بنفسك .. كما سنتعرض أيضاً فى هذا الفصل إلى حساب الضيف أو Guest وما يمكن أن يسببه لنا مشاكل بسبب عدم قيام ميكروسوفت بوضع قيود مباشرة على هذا الحساب .

كيف يتم إختراق الويندوز من خلال ال Administrator ؟؟

حساب الــ Administrator لا يظهر فــى شاشــة الــدخول العادية للويندوز ويتم الدخول له بأحد الطرق الأتية :

الطريقة الأولى :

عند بداية تشغيل الويندوز قم بالضغط بإستمرارعلى مفتاح F8 من لوحة المفاتيح ليظهر لك الشكل التالى :

```
indows Advanced Options Menu
lease select an option:

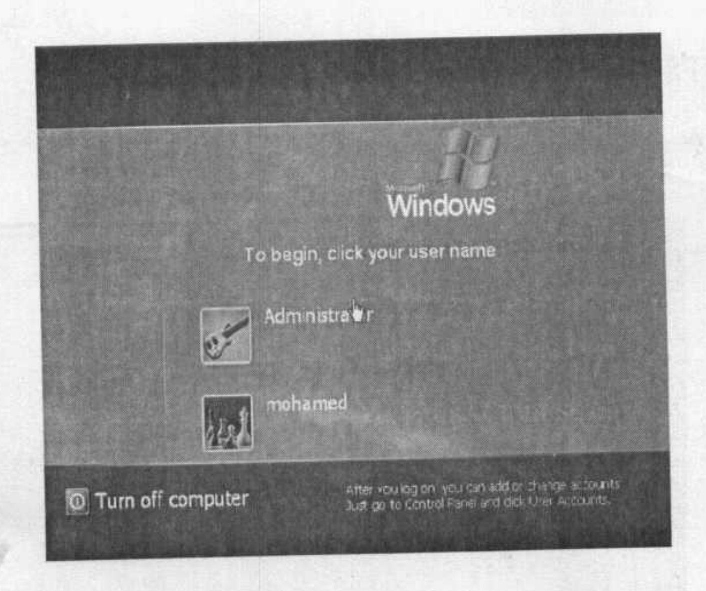
   Safe Mode
   Safe Mode with Networking
   Safe Mode with Command Prompt

   Enable Boot Logging
   Enable VGA Mode
   Last Known Good Configuration (your most recent settings that worked)
   Directory Services Restore Mode (Windows domain controllers only)
   Debugging Mode
   Disable automatic restart on system failure

   Start Windows Normally
   Reboot
   Return to OS Choices Menu

se the up and down arrow keys to move the highlight to your choice.
```

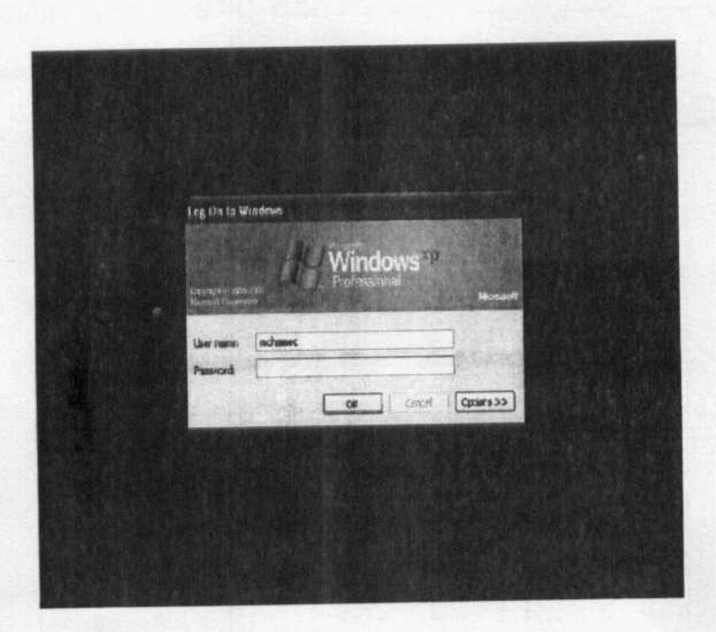
من الشكل السابق تحرك بالأسهم لكى تصل إلى الإختيار Safe Mode أو الوضع الأمن ثم قم بالضغط على مفتاح Enter وأنتظر حتى يظهـــر لك الشكل التالى :



كما تلاحظ فى الشاشة السابقة يظهر لك المستخدمين الذين لهم حـــساب على الجهاز وتجد أنـــه قـــد ظهـــر أيـــضاً الحـــساب الخـــاص بـــال Administrator ويمكنك الأن الضغط عليه بالماوس فإن كان لا يوجد كلمة مرور له فسيتم الدخول للويندوز مباشرة .

الطريقة الثانية :

عند بداية تشغيل الجهاز وظهور الشاشة الخاصة بإدخال كلمة المرور الخاصة بالمستخدم العادى قم بالضغط على مفاتيح ctr + Alt ثم Delete مرتين لتظهر لك نافذة دخول الويندوز الكلاسيكية الخاصة بالإصدارات السابقة كما بالشكل التالى :



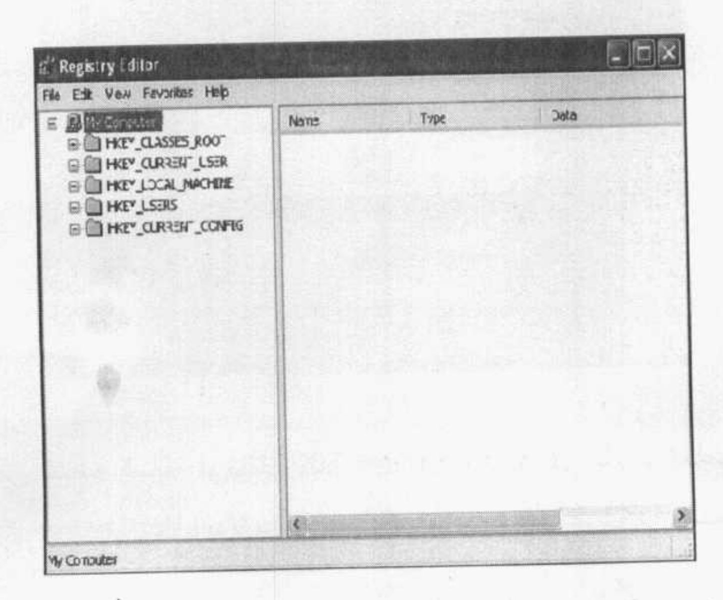
من الشاشة السابقة قم بكتابة كلمة Administrator فى الجزء الخاص بال User name بدلا من الإسم المكتوب ثم اضغط على OK وستجد

نفسك داخل الويندوز هذا بالطبع إذا لم يكن هناك كلمة مـــرور خاصـــة بال Administrator .

إظهار حساب Administrator دائماً فى شاشة الدخول للويندوز :

يمكنك بإتبـــاع الطريقـــة التاليـــة أن تقـــوم بإظهـــار حـــساب Administrator دائما فى شاشـــة الـــدخول إلـــى الوينـــدوز كبـــاقى المستخدمين .

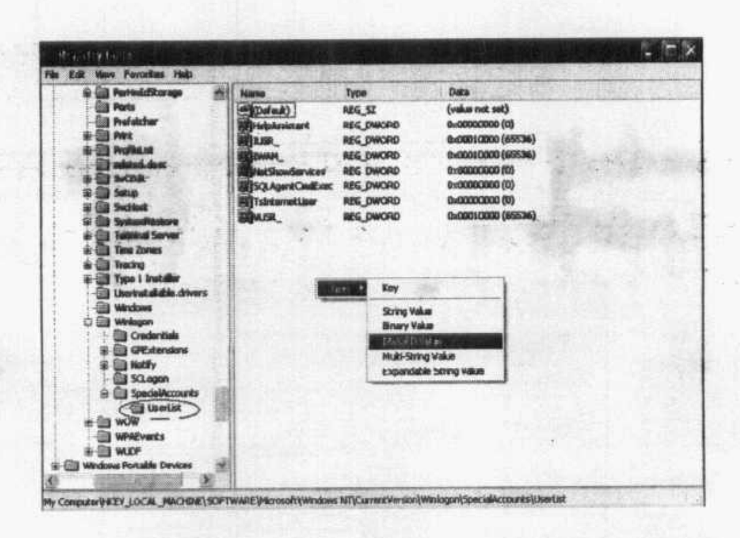
قم بفتح صندوق Run من قائمة start وأكتب داخله Regedit لتفـــتح لك نافذة محرر السجل كما بالشكل التالى :



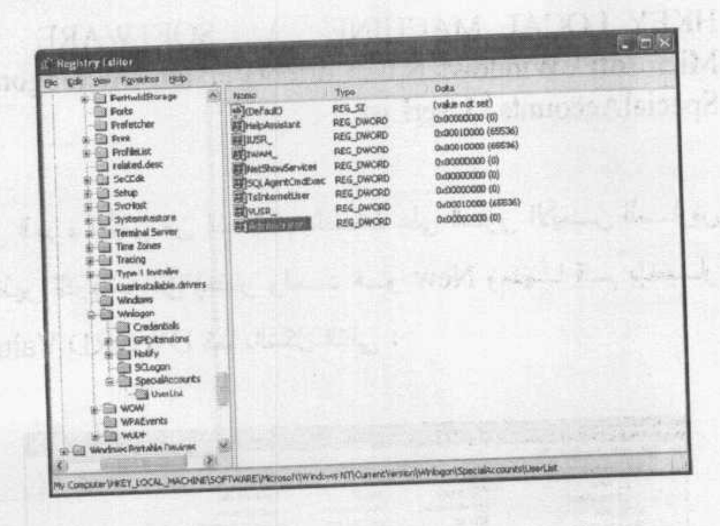
قم بالذهاب إلى المسار التالى :

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon \ SpecialAccounts \ UserList

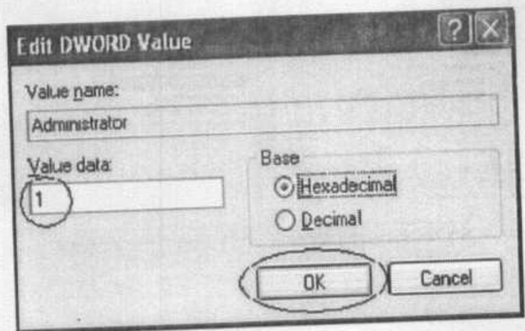
فى الجزء الأيمن من النافذة قم بالضغط على الـزر الأيمـن للمـاوس لتظهر لك قائمة من إختيار واحـد هـو New ومنهـا قـم بإختيـار DWORD Value كما بالشكل التالى :



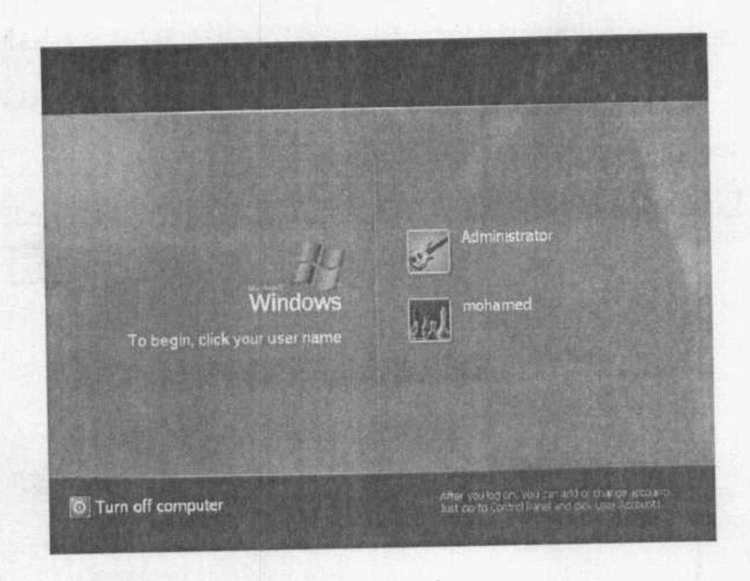
ثم قم بتسمية هذه القيمة الذى قمت بإنـــشائها بالإســـم Administrator كما يلى :



قم بالضغط بالماوس مرتين على هذه القيمة ليظهر لك صندوق الحـــوار التالى :



قم بتغير القيمة إلى 1 ثم أضغط OK كما موضح بالشكل السابق وبذلك ستجد حساب Administrator دائماً فى شاشة دخول الويندوز بجـوار باقى المستخدمين كما بالشكل التالى :

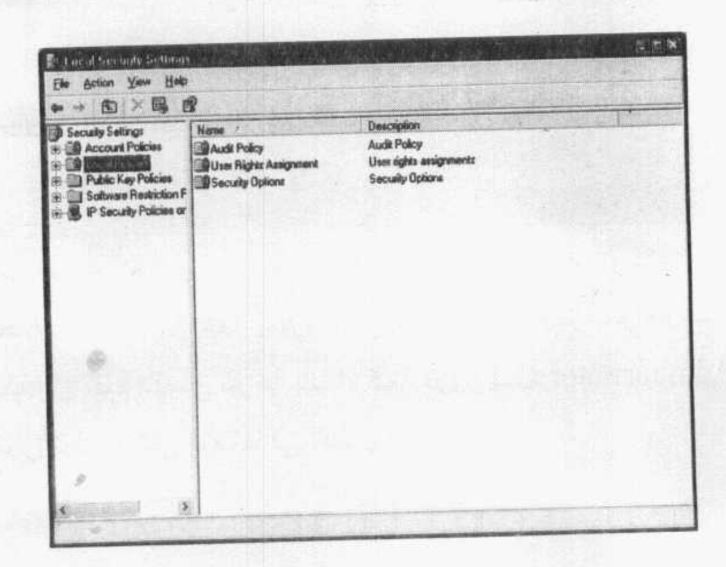


بعد أن عرفت الأن كيف يمكن الدخول بسهولة إلى جهازك وإختراقـه عليك أن تقوم بأقصى سرعة بإنشاء كلمة مرور لـــل Administrator بنفس الطريقة التى إتبعناها فى الفصل السابق .

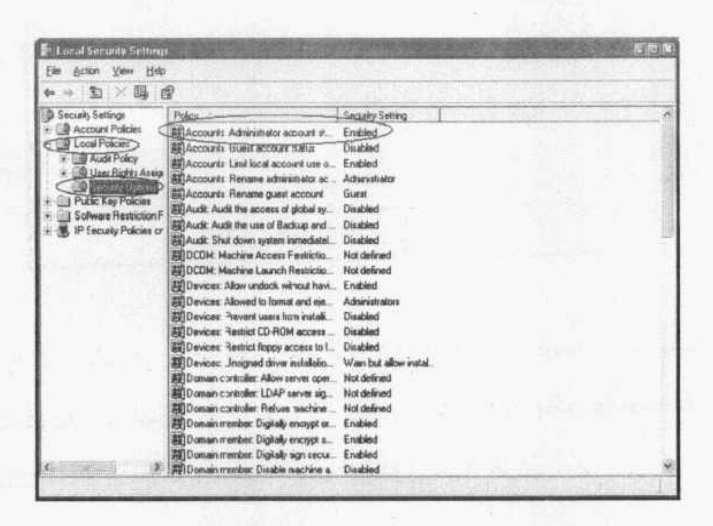
إخفاء Administrator من شاشة الدخول إلى الويندوز فى كل الأحوال ! :

يمكنك بهذه الطريقة أن تقوم بإخفاء حـــساب Administrator من شاشة دخول الويندوز وتجعله لا يظهر حتـــى وإن قمـــت بـــإجراء الخطوات السابقة الخاصة بإظهار حساب Administrator عن طريق محرر السجل Registry !!!

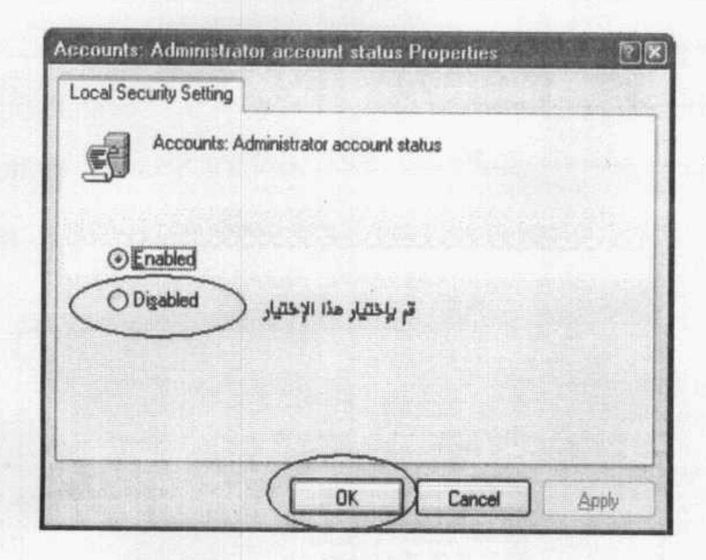
قم بفتح صندوق من قائمة start ثم أكتب الأمر secpol.msc داخله واضغط الزر OK لتظهر لك نافذة Local Security Settings الخاصة بالتعامل مع نظام التأمين كما بالشكل التالى :



فى الجانب الأيسر من النافذة السابقة قم بالضغط مرتين علـــى المجلـــد Local Policies لتتفرع منه عدة تفريعات قم بالضغط علـــى المجلـــد Security Options منها لتظهر لك فى الجهة اليمنى التحكمات التـــى يتيحها هذا الإختيار كما بالشكل التالى :



فى الجانب الأيمن من النافذة ستجد من بين الإختيارات والتحكمات التى ظهرت لك الاختيـــار الأول Accounts:Administrator account status كما مبين لك بالشكل السابق قم بالـــضغط مـــرتين فـــوق هـــذا الإختيار لتظهر نافذة الحوار التالية :



ستجد أن الإختيار الإفتراضى هو Enabled فقـم بإختيـار الوضـع Disabled ثم اضغط فوق الـزر Ok وبـذلك لـن يظهـر حـساب Administrator فى شاشة دخول الويندوز مرة أخرى .

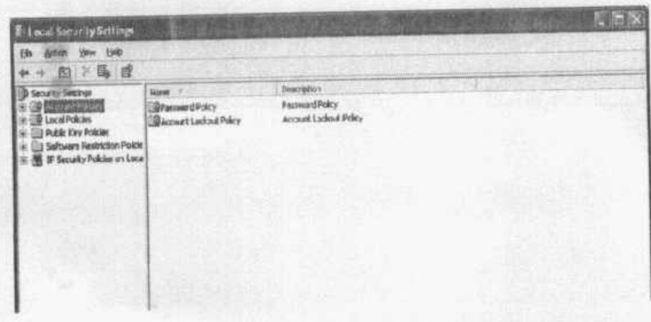
هل هذا يكفى ؟؟؟

قد تعتقد الأن أن الويندوز لديك أصبح سد منيع أمام أى محاولة لإختراقه ولكن أقول لك وللأسف أن تطور برامج الأختراق والطـرق المتبعة فى ذلك تجعلنا لا نطمئن كثيراً وسأذكر لك مثالاً لما يمكـن أن

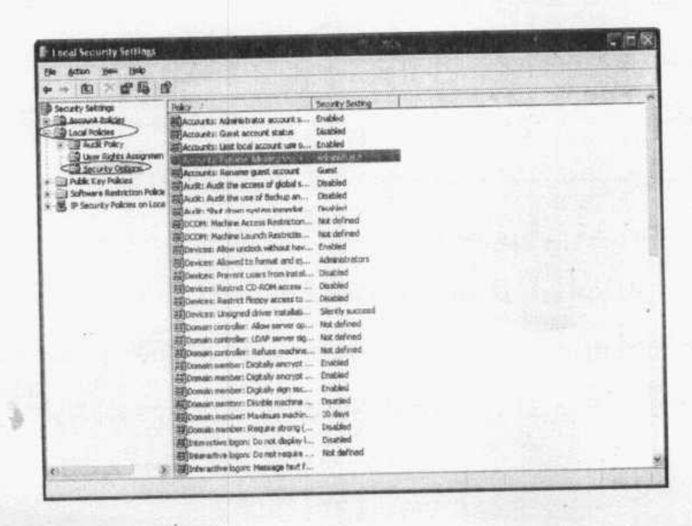
يمثل تهديداً بالنسبة لنا .. فأنت عند إتصالك بالإنترنت تكون عرضة لبرامج الإختراق المتنوعة ..

وأسألك سؤالاً أخر وهو ما الذى يحتاج إليه المخترق للدخول إلى أى جهاز كمبيوتر ؟ بالطبع يحتاج إلى شيئين .. اسم المستخدم وكلمة المرور الخاصة به .. وبما أن الاسم Administrator هو اسم موحد فى جميع أنظمة الويندوز فبذلك يكون المخترق قطع نصف الطريق فى الوصول إلى غايته وفى الجزء الأخر يقوم بإستخدام أحد البرامج الخاصة بتجربة كلمات المرور ... وهذه الطريقة من أشهر الطرق المستخدمة الأن فى الإختراق وعليه سنقوم هنا بقطع هذا الطريق على هؤلاء المخترقين وإرجاعهم مرة أخرى إلى خط البداية وذلك بتغيير اسم Administrator المتعارف عليه إلى أى اسم أخر.

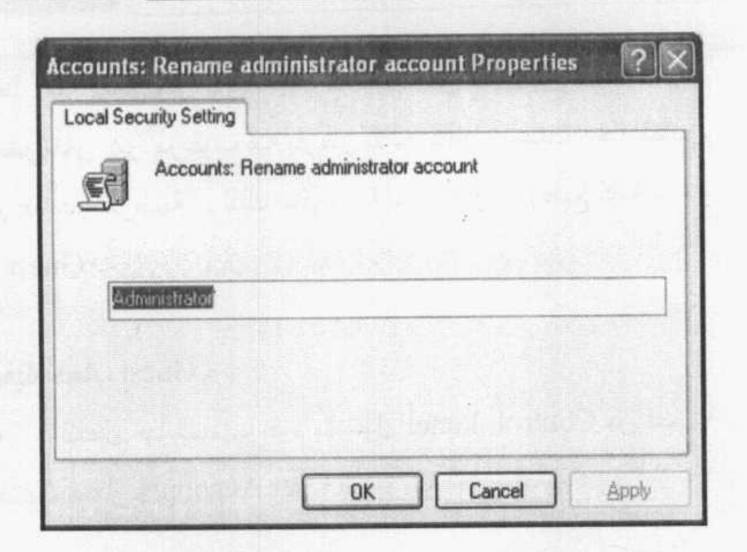
قم بفتح صندوق Run من قائمة start وأكتب داخله secpol.msc للدخول إلى نافذة Local Security Settings مرة أخرى كما بالشكل التالى :



من النافذة السابقة قم بالضغط مرتين على Local Policies لتتفرع منه عدة تفريعات قم بالضغط على الخيار Security Options منها لتظهر لك فى الجهة اليمنى التحكمات التى يتيحها هذا الإختيار ثم قم بالبحـث بينها عــن الإختيــار Accounts: Rename administrator كمـا بالشكل التالى :



بعد أن تجد هذا الخيار قم بالضغط عليه مرتين لتظهر لك النافذة التالية:



من النافذة السابقة يمكنك حذف كلمة Administrator وكتابة الإسم الجديد الذى تريده والضغط على OK لتكون بذلك قد قطعت شوطاً كبيراً من مراحل تأمين الويندوز .

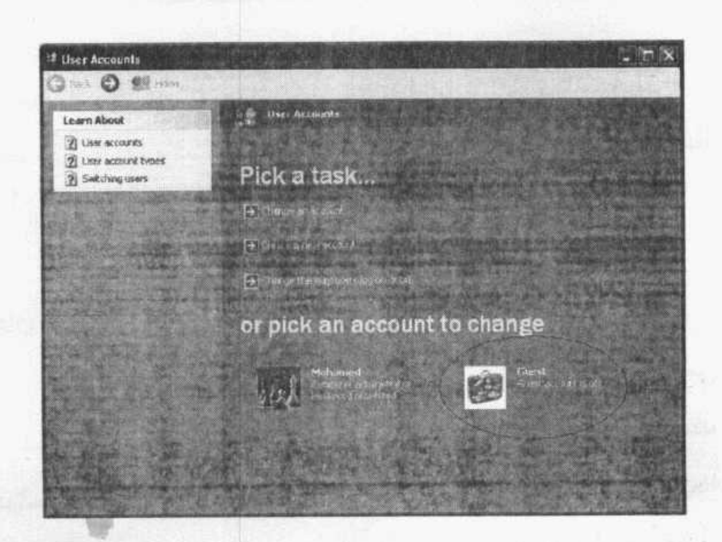
حساب الضيف Guest :

قامت ميكروسوفت بإضافة هذا الحساب للتيسير على المستخدمين فى حالة أراد أحد الضيوف التجول داخل الويندوز وذلك بصلاحيات محدودة جداً ولكنها لم تقم بإتاحة وضع كلمة مرور لهذا الحساب بطريقة مباشرة ولا ندرى هل لذلك علاقة بكرم الضيافة أم يوجد سبب أخر ؟! ولكن منطقياً أعتقد أن ذلك هو السبب ولكنه سبب قد

يكلفنا الكثير حتى وإن كان هؤلاء الضيوف من الذين نثق فيهم فقد يقوم شخص أخر غير مرغوب فيه بفرض نفسه عليك وإستغلال هذا الكــرم بطريقة غير مرضية .. لذلك سنقوم هنا بمعرفة كيفية وضع كلمة مرور لل Guest .

تشغيل حساب Guest :

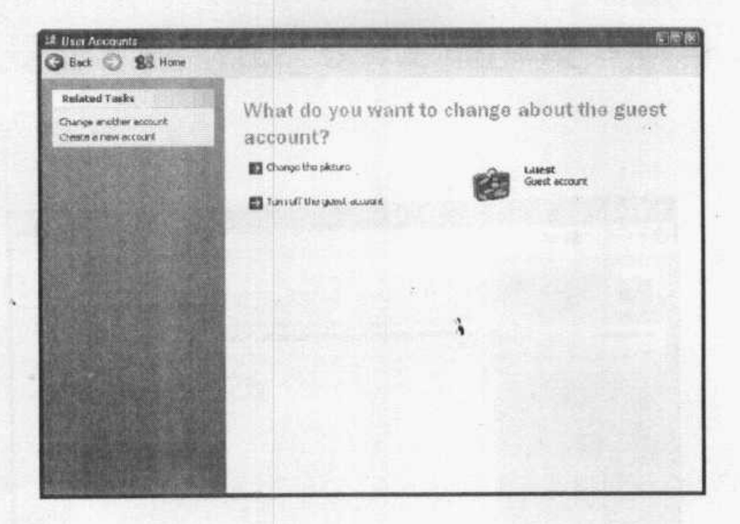
لتفعيل هذا الحساب نقوم بالدخول Control Panel من قائمــة start ثم نختار User Accounts لتظهر لنا النافذة التالية :



قم بالضغط على Guest المشار إليه بالشكل السابق لتظهر لك النافـذة الأتية :



قم بالضغط على Turn On the Guest Account من النافذة السابقة ليتم تفعيل حساب الضيف وتختفى هذه النافذة والعودة إلى النافذة السابقة لها وعند الضغط على Guest مرة أخرى ستظهر لك نافذة التحكم فـى إعدادات الحساب Guest كما بالشكل التالى :



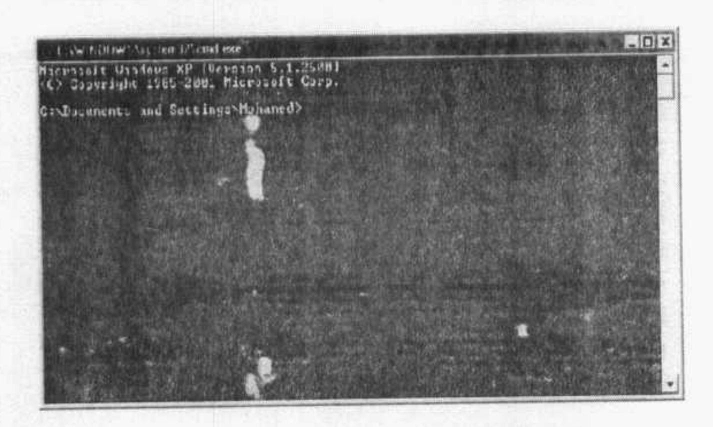
كما ترى من الشكل السابق إن الإختيارات المتاحة للـتحكم فـى هـذا الحساب تكاد تكون معدومة ولا تتيح لك إمكانية وضع كلمة مرور لـه ولذلك لكى نقوم بوضع كلمة مرور لهذا الحساب سنتبع طـرق أخـرى مختلفة عن الطرق التقليدية .

وضع كلمة مرور لحساب Guest :

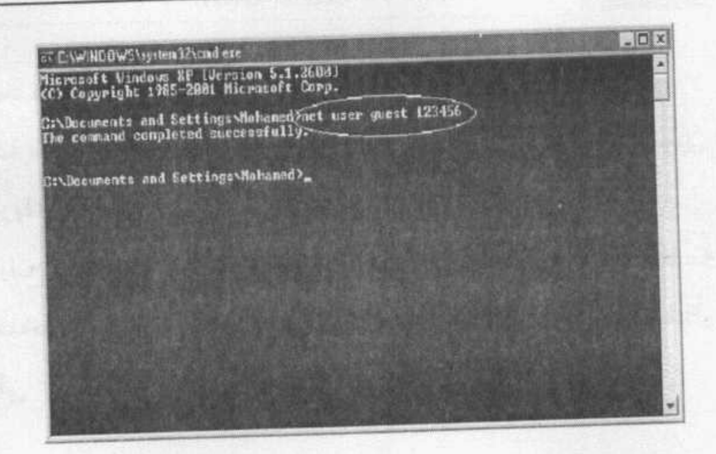
يمكنا الأن أن نضع كلمة مرور لهذا الحساب بأى من الطريقتين الأتيتين

الطريقة الأولى :

قم بفتح صندوق Run من قائمة start ثـم قـم بكتابـة cmd دلخلـه وأضغط Ok لفتح موجه الأوامر command prompt كمـا بالـشكل التالى :



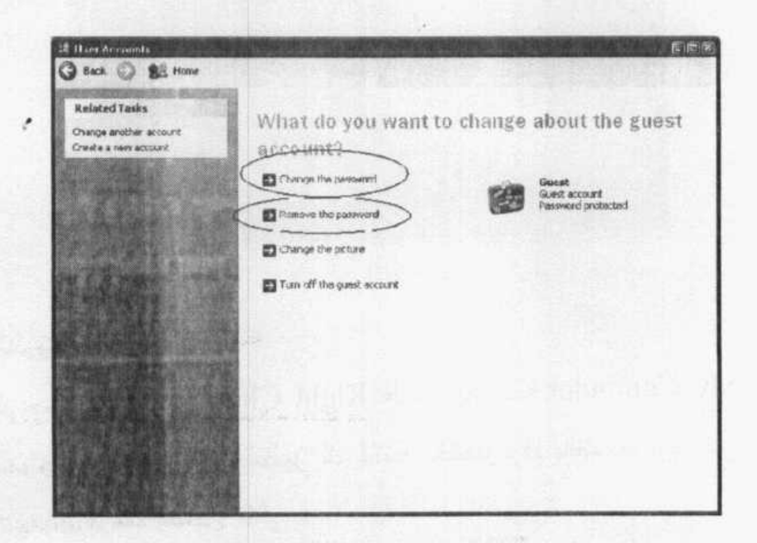
من خلال محث الدوس قم بكتابـة net user guest password ثـم أضغط Enter مع ملاحظة أن password هى كلمـة المـرور فقـم بالتعويض عنها بالكلمة التى تريدها .



والأن عند محاولة أحد للدخول عن طريق حساب guest لن يتمكن من ذلك قبل إدخال كلمة المرور كأى مستخدم عادى كما بالشكل التالى .



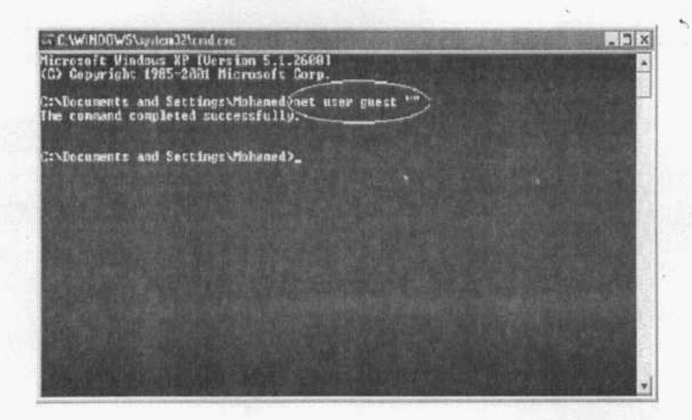
والأن عند الرجوع إلى حساب guest من نافذة User Accounts مرة أخرى ستجد الإختيارات قد إختلفت كما بالشكل التالى :



حذف كلمة مرور حساب Guest :

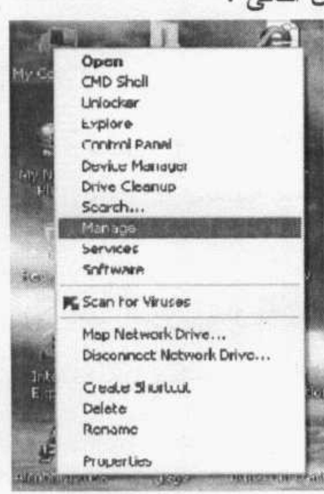
1- يمكنك حذف كلمة المرور حساب الـضيف guest بالطريقـة العادية بعد إضافة الإختيارات الخاصة بذلك كما هو موضح لك بالشكل السابق .

2- يمكنك أيضاً حذف كلمة المرور بطريقة أخرى وذلك بالـذهاب إلى محث الدوس مرة ثانية واكتب "" net user guest ثـم اضغط Enter كما بالشكل التالى .

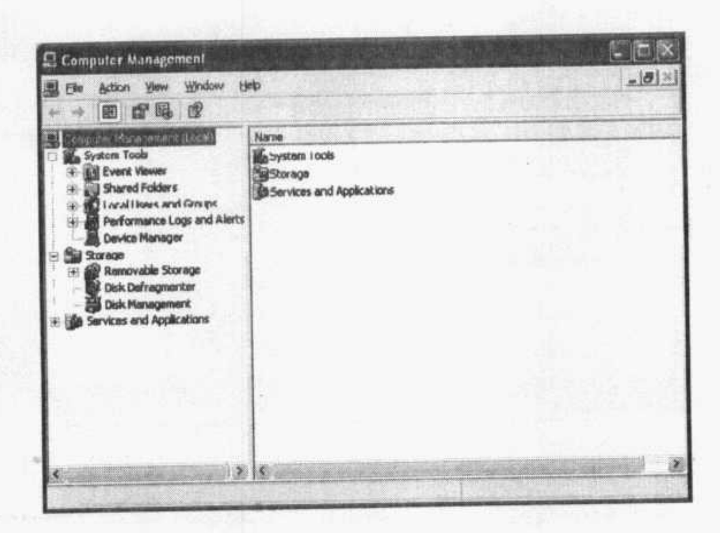


الطريقة الثانية :

قم بضغط المــاوس Right Click علــى أيكونــة My Computer الموجودة بسطح الكتبب لتظهر لك قائمة مختصرة قم بالضغط فيها على Manage كما بالشكل التالى :

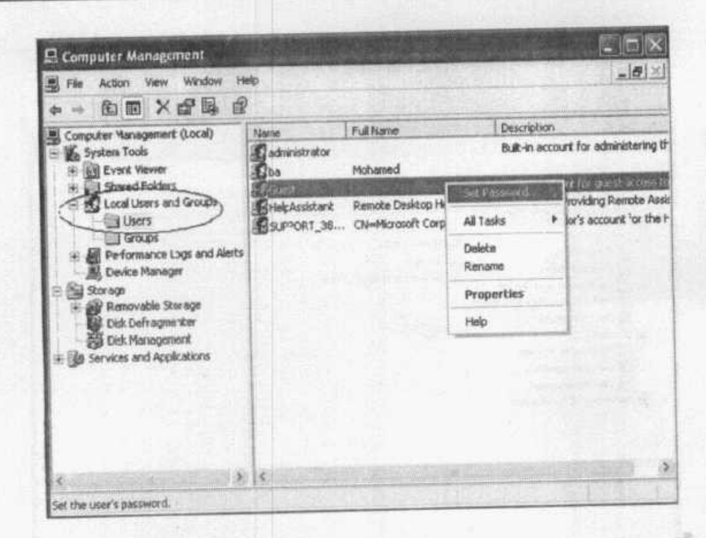


لتظهر لك النافذة التالية :

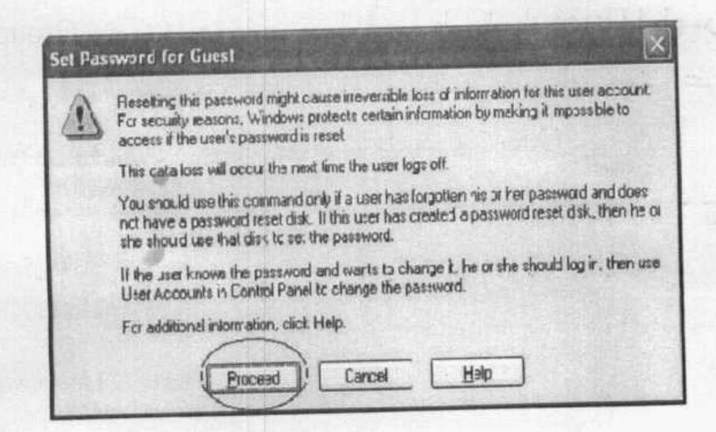


من النافذة السابقة قـم بالـضغط مـرتين علـى Local Users and Groups ليتفرع منها مجلدين قم بالوقوف على المجلد Users ليظهـر لك فى الجهة اليمنى من النافذة أسماء المستخدمين الذين لهم حساب على الويندوز ومن بينها الحساب الخاص بالضيف أو Guest .

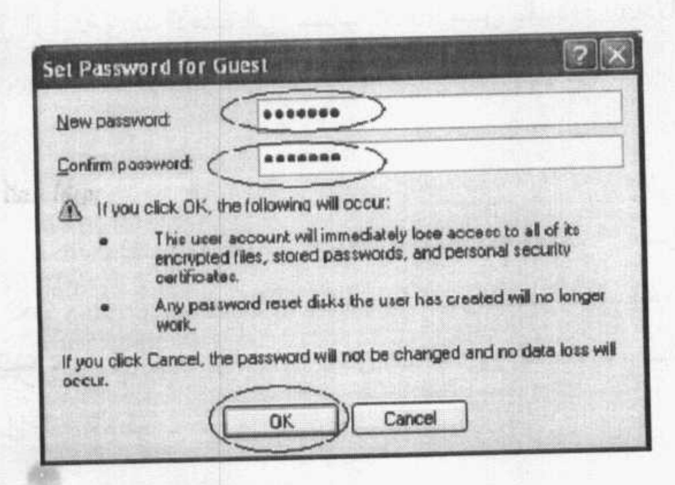
قم بالضغط عليه بزر الماوس الأيمن لتظهر لك قائمة مختـصرة كمـا بالشكل التالى :



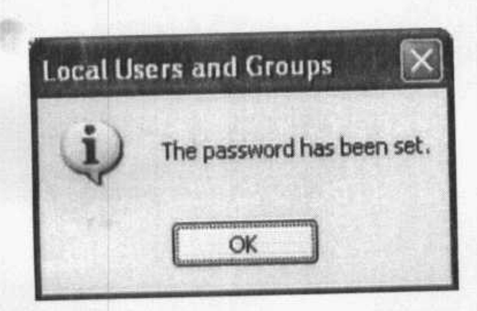
من النافذة السابقة بالضغط على Set Password من القائمة المختصرة لتظهر لك الرسالة الأتية :



قم بالضغط على Proceed من الرسالة السابقة لتظهر النافذة التالية :



من النافذة السابقة قم بإدخال كلمة المرور التى تريدها فى الخانة الأولى ثم أعد كتابتها مرة أخرى فى الخانة الثانية ثم أضغط Ok لتظهـــر لـــك الرسالة التالية :



تخبرك الرسالة السابقة بإنشاء كلمة المرور قــم بالــضغط علـــى Ok لإغلاق الرسالة وعند الذهاب إلى حساب guest مــن نافــذة User Accounts ستجد الإختيارات أيضاً قد إختلفت كما بينا من قبل .

حذف كلمة المرور :

يمكنك حذف كلمة المرور أو تغييرها بالطريقة العاديــة مــن خلال نافذة User Accounts أو يمكنك إعادة نفس الخطوات الــسابقة مرة أخرى إلى أن تصل إلى خطوة إدخال كلمة المرور فلا تكتب شــيئاً ثم أكمل باقى الخطوات كما هى .

الفصل الثالث

مزيد من الأمان

مزيد من الأمان

سنتعرض فى هذا الفصل إلى الطرق التى تمكنا من احكام السيطرة على الويندوز من خلال إستغلال عدد من الخدمات التى يتيحها لنا نظام التشغيل والتى يمكن من خلالها فرض الكثير من القيود والتحكمات للحصول على أكبر قدر من الأمن والحماية مثل إخفاء أحد المستخدمين من شاشة الدخول إلى الويندوز كما سنتناول كيفية تفعيل كلمات المرور كأن نجعل الويندوز يقوم بفرض عدد من الشروط عند إنشاء كلمات المرور تضمن لنا كلمات مرور معقدة يصعب معها مهمة أى شخص يحاول إكتشافها أوتوقعها وغير ذلك من الأشياء التى يمكن أن تكون مفيدة بالنسبة لنا .

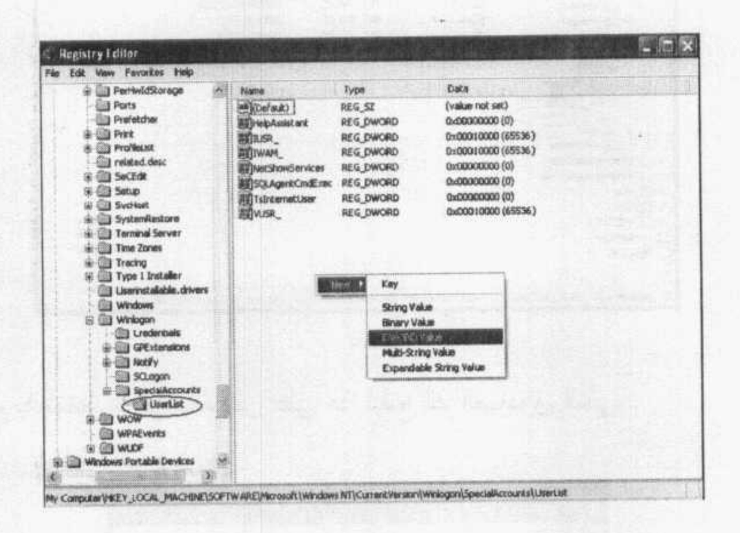
إخفاء مستخدم من شاشة دخول الويندوز :

يمكنك إخفاء أى مستخدم له حساب فى الويندوز وتجعله لا يظهر فى شاشة دخول الويندوز بإتباع الخطوات التالية :

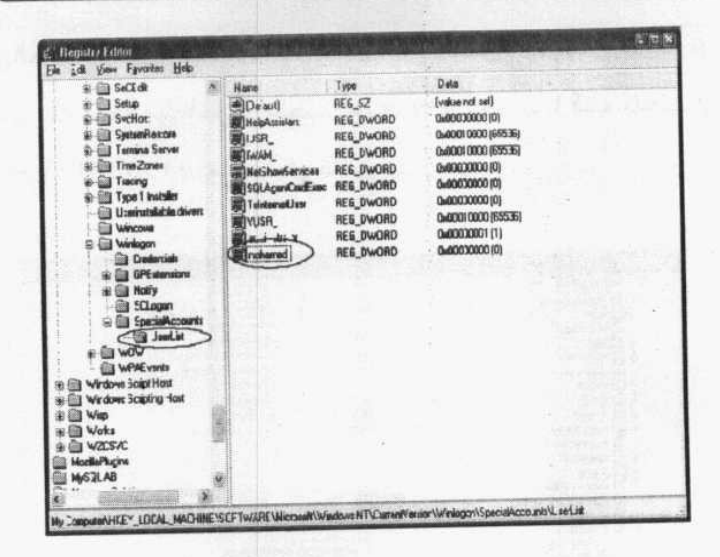
قم بالذهاب إلى المسار التالى :

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon \ SpecialAccounts \ UserList

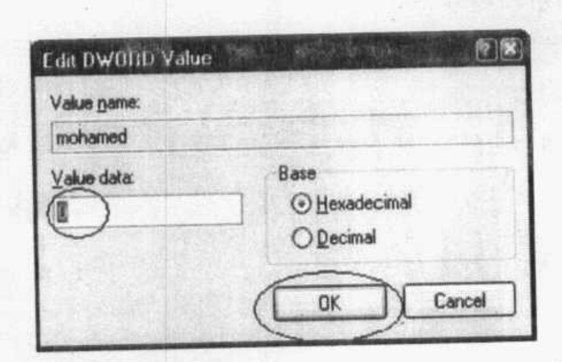
فى الجزء الأيمن من النافذة قم بالضغط على الـــزر الأيمـــن للمـــاوس لتظهر لك قائمة من إختيار واحـــد هـــو New ومنهـــا قـــم بإختيـــار DWORD Value كما بالشكل التالى :



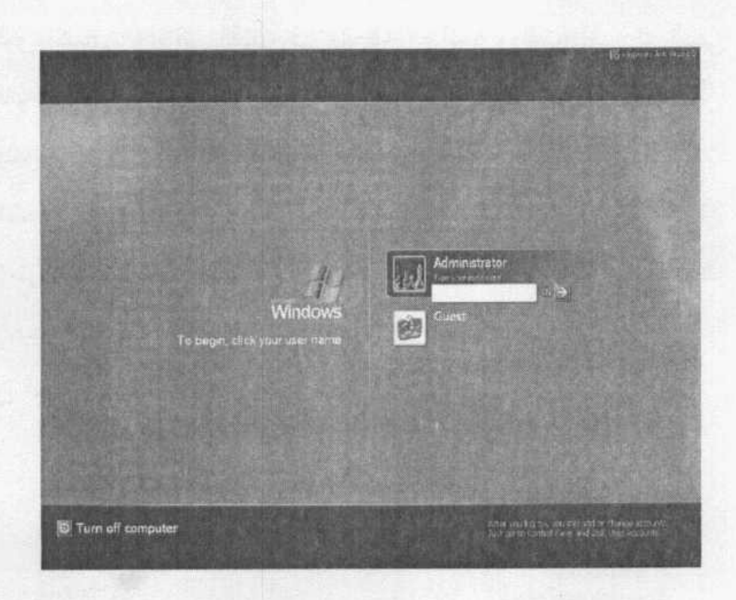
ثم قم بتسمية هذه القيمة الذى قمت بإنشائها باسم المستخدم الـــذى تريـــد إخفاءه كما يلى:



قم بالضغط مرتين بالماوس على هذا ليفتح لك الصندوق التالى :



ستجد أن القيمة الإفتراضية هى (0) اتركها كمـا هـى واضـغط OK والأن فى المرة القادمة لدخولك الويندوز لن يظهر أسم هذا المـستخدم كما بالشكل التالى :

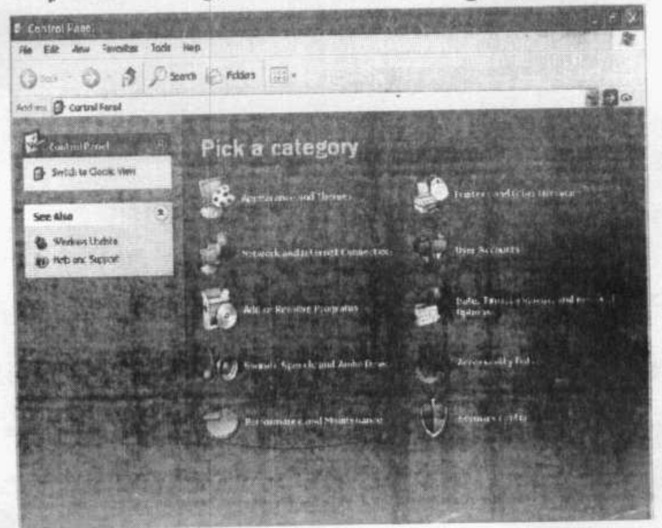


جعل كلمات المرور أكثر فاعلية :

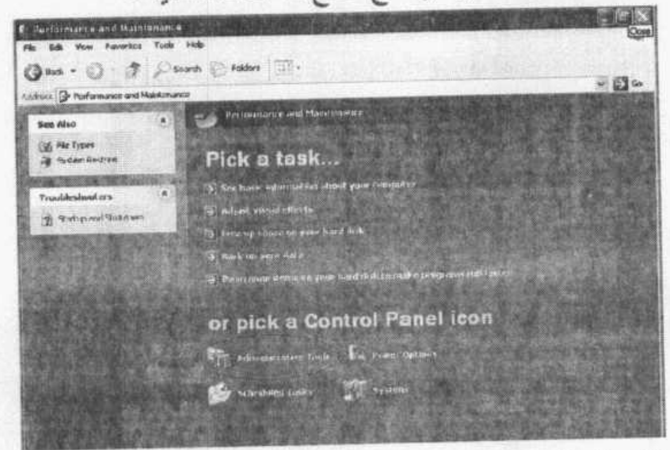
كلمات المرور هى المفتاح الأمين الـذى نـستخدمه لإغـلاق الويندوز فى وجه لصوص المعلومات والمتطفلين ويجب أن نهتم بـأن يكون هذا المفتاح من النوع الجيد فليس من المعقول بعد كل ما قمنا بـه من مجهود لتأمين خصوصياتنا من أيدى هؤلاء العابثين أن لا نهتم فـى

النهاية بالإختيار الجيد لكلمات المرورهذه و نقوم بوضع كلمات سر سهلة و بسيطة تجعل هؤلاء الأشرار يودوا لو أن يقدموا لنا الشكر على معاونتا الصادقة و المخلصة لهم فى إنجاح مخططاتهم !!! فأرجو أن أكون بكلماتى هذه قد أنقذتك فى اللحظة المناسبة و لفت نظرك إلى أهميه هذه النقطة ... ومن أجل أهمية هذا الموضوع وخطورته تجد أن ويندوز اكس بى يمد لك يد العون فيه ويتيح لك العديد من الإمكانات والتحكمات من أجل الوصول إلى أعلى مستوى ممكن من الأمان والسرية وسنقوم فى هذا الجزء من الكاتب بإستعراض أهم تلك الإختيارات وكيفية الإستفادة منها .

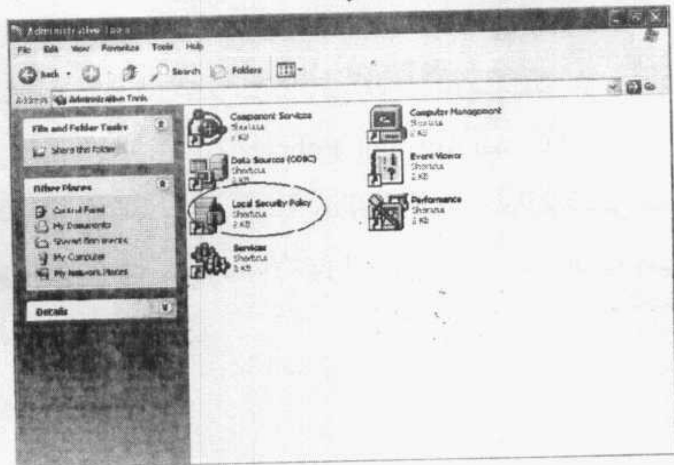
من قائمة start قم بفتح Control Panel لتظهر لنا النافذة التالية :



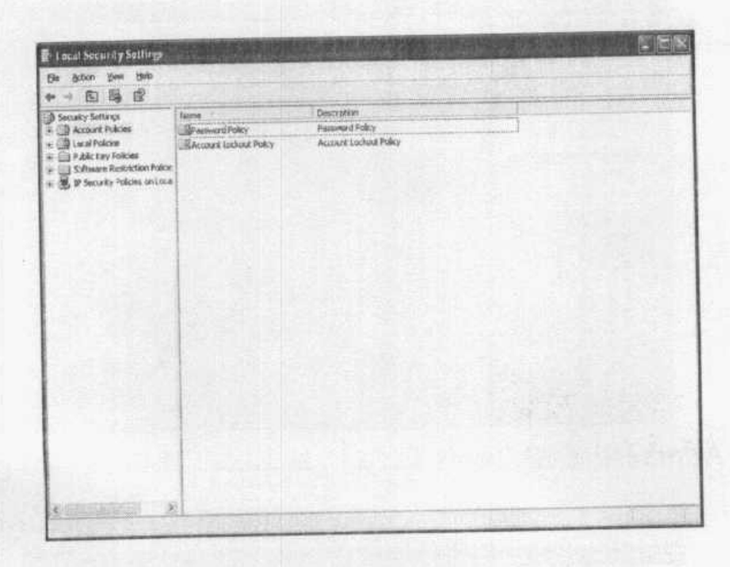
من النافذة السابقة قم بالـــضغط علـــى أيكونـــة Performance and Maintenance كما هو موضح لتفتح لنا النافذة التالية :



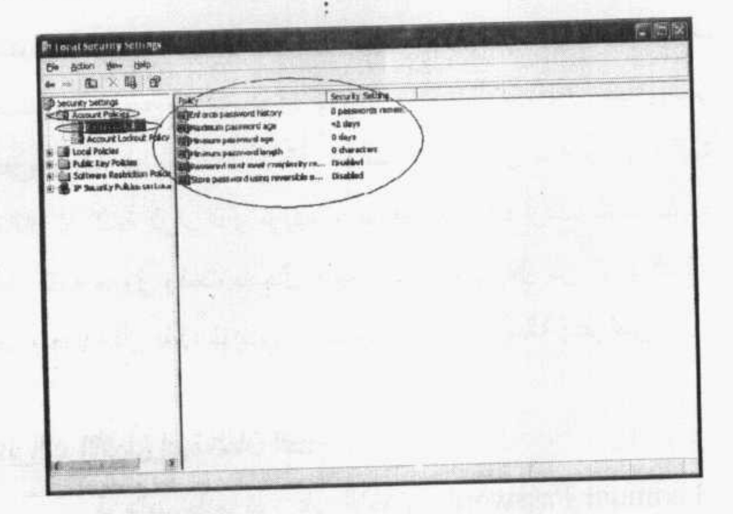
من النافذة السابقة قم بالضغط على أيكونـــة Administrative Tools الموضحة لك لتظهر لك النافذة التالية :



من النافذة السابقة قم بالضغط مرتين على أيكونـــة Local Security Policy الخاصة بالتعامل مع سياسة التأمين لتفتح لنا النافذة الأتية :

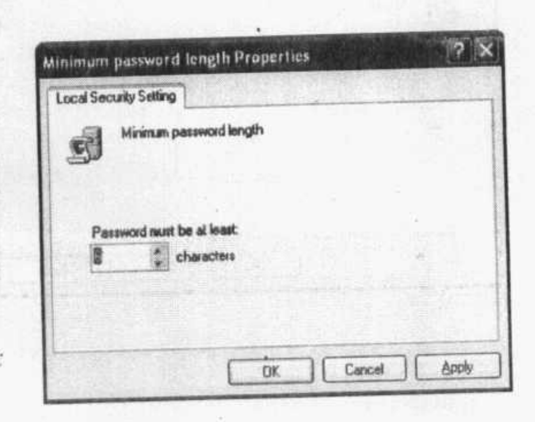


من النافذة السابقة التى ظهرت لك وفى الجانب الأيسر منها قم بالضغط مرتين بالماوس على أيكونة Account Policies لتجد أنه تفرع منهـــا أيكونتان قم بالضغط على أيكونـــة Password Policy ليظهـــر فـــى الجزء الأيمن النافذة مجموعة الإختيارات التى ســنتعامل معهـــا كمـــا بالشكل التالى :



تحديد عدد حروف كلمات السر :

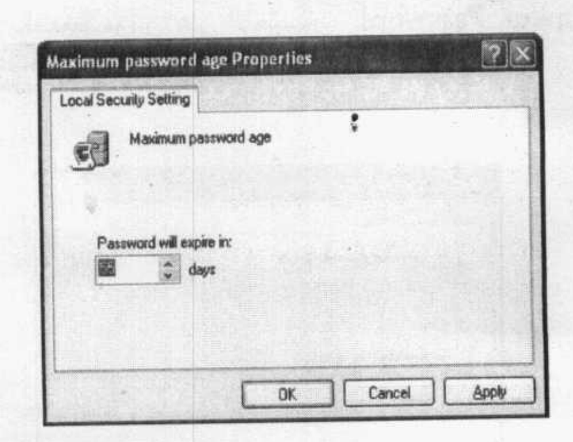
قم بالضغط مرتين على الإختيـــار Minimum Password length لتظهر لك النافذة التالية :



صندوق الحوار السابق هو المسئول عن تحديد الحد الأدنى لعدد حروف كلمات السر ويتيح لك الويندوز الإختيار ما بين 1 إلى 14 رقم ومن المعروف أنه يفضل دائما ألا تقل كلمات المرور عن ستة أرقام .. قم بإختيار أو كتابة الرقم الذى تريده ثم أضغط ok وإذا أردت بعد ذلك إنشاء كلمة مرور وقمت بإدخال كلمة عدد حروفها أقل من العدد الذى قمت بتحديده فلن يقبل الويندوز بذلك وسيظهر لك رسالة إعتراض .

تحديد الحد الأقصى لفترة كلمات السر :

قم بالضغط مرتين على الإختيار Maximum Password age لتظهر لك النافذة التالية :

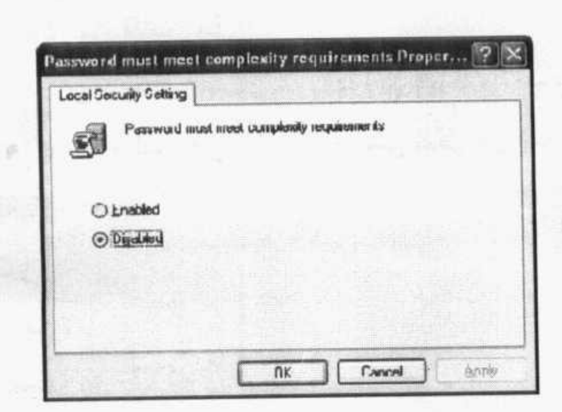


من الصندوق السابق قم بتحديد عدد الأيام التى ينتهى عندها فاعلية كلمة السر ويطالبك الويندوز بتغييرها ثم أضغط Ok .

لاحظ : أيضاً أنه يوجد خيار باسم Minimum Password age عكس الإختيار السابق وهو مسئول عن تحديد الحد الأدنى للأيام التى تنتهى بعدها فاعلية كلمات المرور وهو يعمل بتكامل بينه وبين الإختيار السابق وعند الضغط عليه يظهر لنا صندوق حوارى شبيه بسابقه ويمكنك التعامل معه بنفس الطريقة .

تحديد مستوى التعقيد فى كلمات السر :

قم بالضغط مرتين على الإختيار Password must meet complexity requirements ليظهر لك النافذة المسئولة عن تشغيل خاصية تعقيد كلمات المرور التالية :



كما ترى بالشكل السابق فإن هذه الخاصية تحتوى على خيـاران الأول Enabled وهو المسئول عن تشغيل وتفعيل هذه الميزة أما الثانى فهـو Disabled لتعطيل هذه الخاصية وهو الوضع الإفتراضى ولكن أعتقـد أن السؤال الذى يدور فى ذهنك الأن هو ما الفرق بـين الإختيـاران ؟! وما الفائدة التى يمكن أن تعود علينا من تشغيل هذه الخاصـية أو عـدم تشغيلها ؟ ولكن قبل أن أجيبك على أسئلتك هذه أريد أن أذكرك بما قلته لك سابقاً عن أهمية كلمات المرور ومدى خطورة أن تكون كلمات سهلة بسيطة ومتعارف عليها ... وذلك لأنك فى الوضع العادى وعندما تكون هذه الميزة معطلة يمكنك أن تقوم بإنشاء أى كلمة مرور تحتوى علـى أى حروف تريدها ولكنك بتشغيل هذه الخاصية وجعلها فـى الوضـع Enabled سيجبرك نظام التشغيل على الإستخدام الأمثل لكلمات الـسر ... بمعنى أنه لا بد أن يتوافر فى كلمة المرور شروط معينـة تحقـق أعلى مستوى ممكن من التأمين مثل :

1- أن لا تحتوى كلمة السر ضمن حروفها اسم صاحب الحساب .

2- أن تحتوى كلمة السر على ثلاثة أنواع على الأقل من البيانـات التالية :

- حروف كبيرة .
- حروف صغيرة .
- علامات خاصة مثل @ أو # .

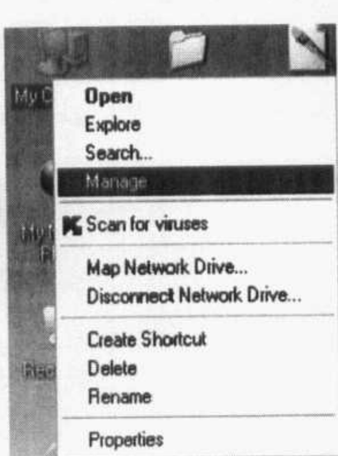
○ أرقام .

أما إذا قمت بإدخال كلمة مرور لا تتوافر فيها تلك الشروط فسيرفض الويندوز ذلك ويظهر لك رسالة إعتراضية كأى صديق مخلص يهتم لأمرك !

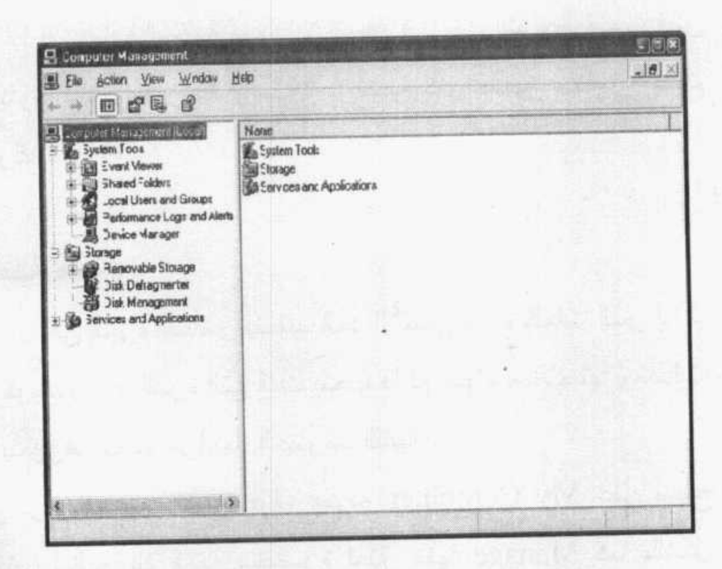
ملاحظة هامة :

فى الجزء الخاص بتحديد الحد الأقصى لفترة كلمات السر إذا لم يقم الويندوز بعد الفترة التى قمت بتحديدها له بإنهاء صلاحيتها ومطالبته لك بتغييرها يمكنك مراجعة الخطوات التالية .

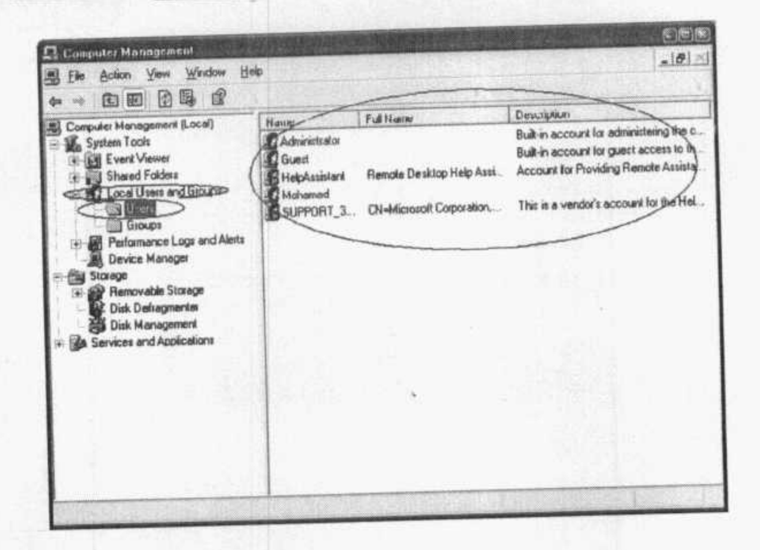
انقر بزر الماوس الأيمن فوق أيكونة My Computer على سطح المكتب لتظهر لك قائمة مختصرة اختار منها Manage كما بالشكل التالى :



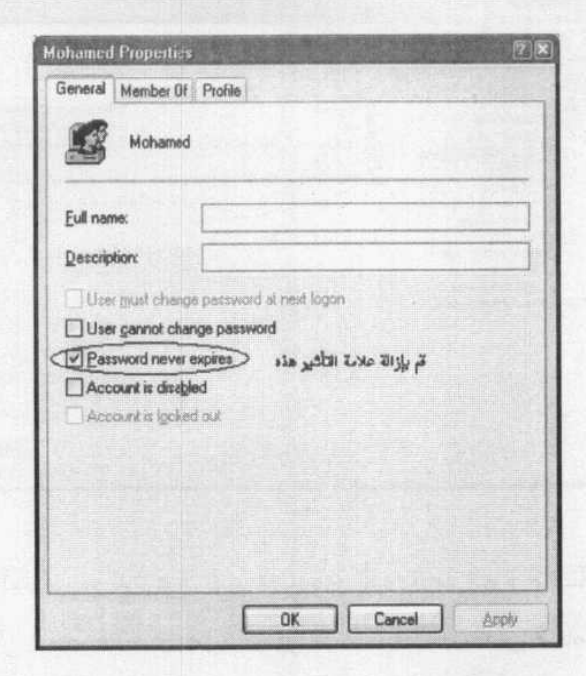
لتظهر لك النافذة التالية :



فى الجانب الأيسر من النافذة السابقة قم بالنقر مرتين بالمـــاوس فـــوق الخيار Local Users and Groups ليتفرع منه مجلدين قـــم بـــالنقر فوق المجلد Users منهم ليظهر لك محتوياته بالجانب الأيمن من النافذة كما بالشكل التالى :



قم بالنقر بالماوس مرتين فوق اسم المستخدم الذى تريد إنهاء صـــلاحية كلمة المرور الخاصة به كل فترة لتظهر لك شاشة الخصائص الخاصـــة به كما بالشكل التالى :



من الشاشة السابقة قم بإزالة علامة التأشير بجوار الإختيار Password never expires كما هو موضح ثم اضغط OK .

الفصل الرابع

مفتاح إقلاع للويندوز

مفتاح إقلاع للويندوز

السطور التالية تسوق إليك مفاجأة غيـر سـارة أو إن أردت الدقة فهى صدمة محبطة ! فبعد كل ما مررنا به وتعلمناه فى الصفحات السابقة من أفكار وخبايا التأمين فى الويندوز تجعلك تزهو بنفسك وبمـا أصبح عليه الويندوز لديك من مستوى تأمين وقدرة على التـصدى لأى محاولة إختراق قد تصعق عندما تعلم أنه يمكن لشخص ما فـى بـضع ثوانى أن يصبح داخل هذا الويندوز يفعل به ما يحلو له ويريده .. فقـد انتشرت فى الأونة الأخيرة على مواقع الإنترت المختلفة نوعيـة مـن البرامج لها القدرة على القيام بذلك بكل سهولة ! وتوجد عدة أنواع مـن هذه البرامج تستخدم بطرق مختلفة ولكن أخطر هـذه الأنـواع علـى الإطلاق هى نوعية من البرامج يمكن تحميلها علـى Cd أو قـرص فلوبى ووضعها داخل الجهاز ليتم الإقلاع من خلالها ثم تظهـر أمامـك على الشاشة قائمة بأسماء جميع المستخدمين الذين لهم حـساب داخـل الويندوز بما فيهم طبعاً حساب Administrator ثـم تقـوم بـالتحرك بالأسهم إلى اسم المستخدم الذى تريد حذف كلمة المرور الخاصـة بـه وتتبع الخطوات !!!

وسنقوم هنا بشرح أحد هذه البرامج وكيفية إستخدامها ولكـن لا بد من التنبيه على أن السبب من شرح مثل تلك البرامج هو الوقـوف على نقاط الضعف والثغرات التى تنفذ منها هذه البرامج وتستغلها داخل

نظام التشغيل حتى يتثنى لنا علاج مثل هذه الثغرات والتغلب عليها وأن ما يهمنا هنا هو الحفاظ عليك وحمايتك وليس الغرض أن تصبح أنـــت أحد هؤلاء الذين نقاومهم !...

برامج حذف كلمات المرور :

سنقوم هنا بإستعمال أحد البرامج التى تعمل من خلال قرص مرن ثم نقوم بتغيير ترتيب الإقلاع ليـــتم الإقـــلاع أولاً مـــن محـــرك الأقراص المرنة Floppy Drive وعند بداية الإقـــلاع وبعـــد وضـــع القرص الذى يحتوى على البرنامج داخل محرك الأقراص تظهـــر لنـــا الشاشة التالية :

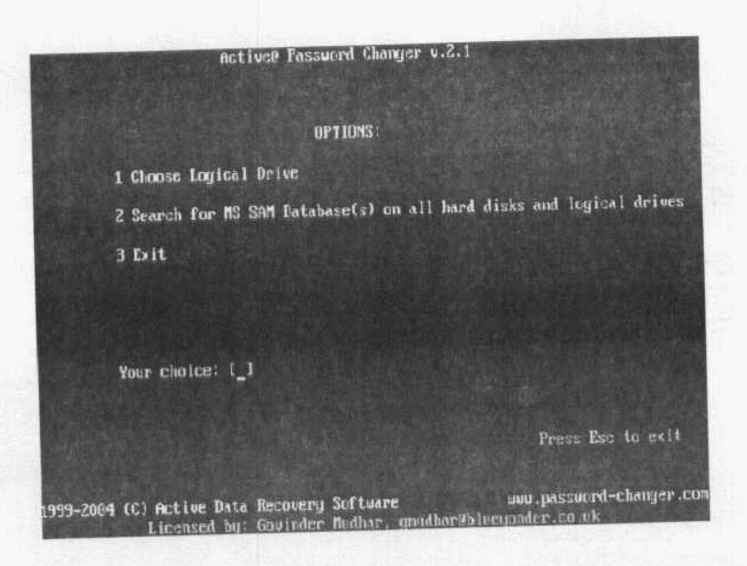
```
FreeDOS kernel version 1.1.35 (Build 2035) [May 30 2004 22:09:36]
Kernel compatibility 7.10 - WATCOMC - FAT32 support

(C) Copyright 1995-2004 Pasquale J. Villani and The FreeDOS Project.
All Rights Reserved. This is free software and comes with ABSOLUTELY NO
WARRANTY; you can redistribute it and/or modify it under the terms of the
GNU General Public License as published by the Free Software Foundation;
either version 2, or (at your option) any later version.
C: HD1, Pri1 1], CHS=    0-1-1, start=     0 MB, size= 16378 MB

[0] Clean boot with Active@ Password Changer
[1] Boot with CD-ROM support
[2] Boot with CD-ROM support and USB support for external HDD
[3] Boot with USB support for external HDD and CD-ROM

Select from Menu [0123], or press [ENTER]- 26 - Singlestepping (F6) is: OFF
```

سنقوم من خلال الشاشة السابقة بإختيار الإختيار الأول كما هو موضح لك وذلك بأن تقوم بضغط الرقم صفر (0) من لوحة المفـــاتيح تــضغط Enter لتظهر لك الشاشة التالية :



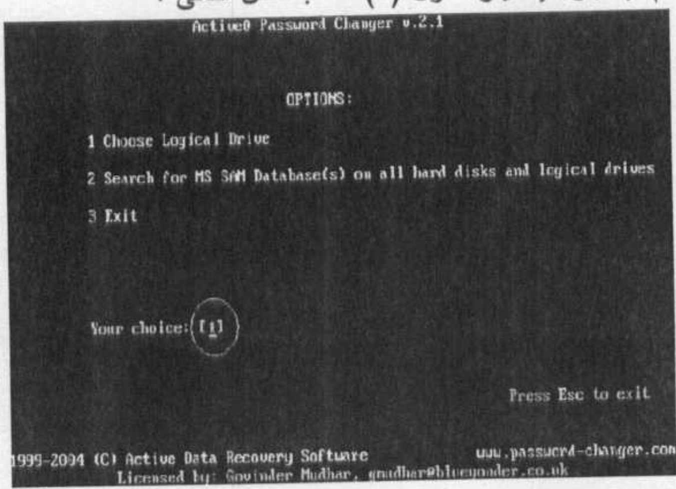
تظهر لك الشاشة السابقة ثلاثة إختيارات :

1- تختار هذا الخيار إذا كنت تعرف القسم أو البارتيشن يوجد بـــه الويندوز .

2- تختار هذا الخيار إذا كنت لا تعرف مكان وجود الويندوز ليقوم البرنامج بالبحث بنفسه عن مكان الويندوز فى داخـــل الهـــارد ديسك .

3- تختار هذا الخيار إذا أردت الخروج من البرنامج .

سأقوم بإختيار الإختيار الأول (1) كما بالشكل التالى :



بعد إدخال الرقم كما مبين وضغط مفتاح Enter تظهر الشاشة التالية :

Active@ Password Changer v.2.1

Logical drives list:

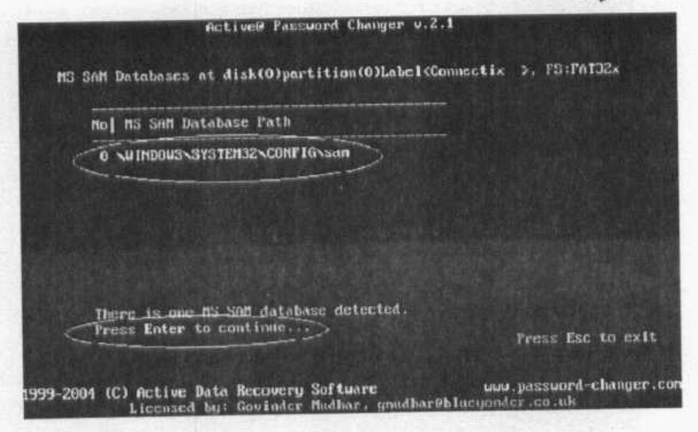
No	HDD	Partition	Type	Disk Label	Size (Mb)
0	(0)	(0)	FAT32x	Connectix	16378

Press Enter to continue...

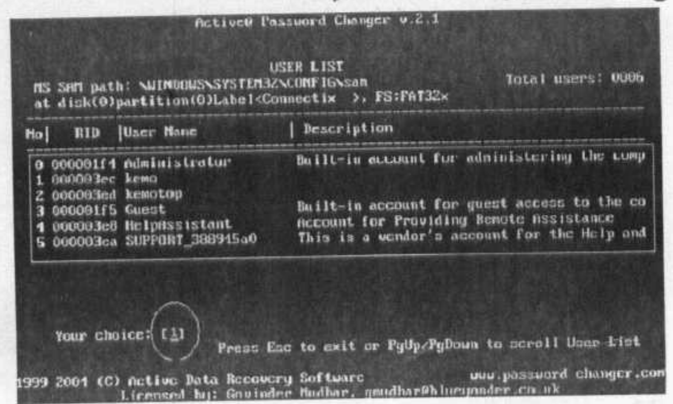
Press Esc to exit

1999-2004 (C) Active Data Recovery Software www.password-changer.com
Licensed by: Govinder Mudhar, gmudhar@bluewonder.co.uk

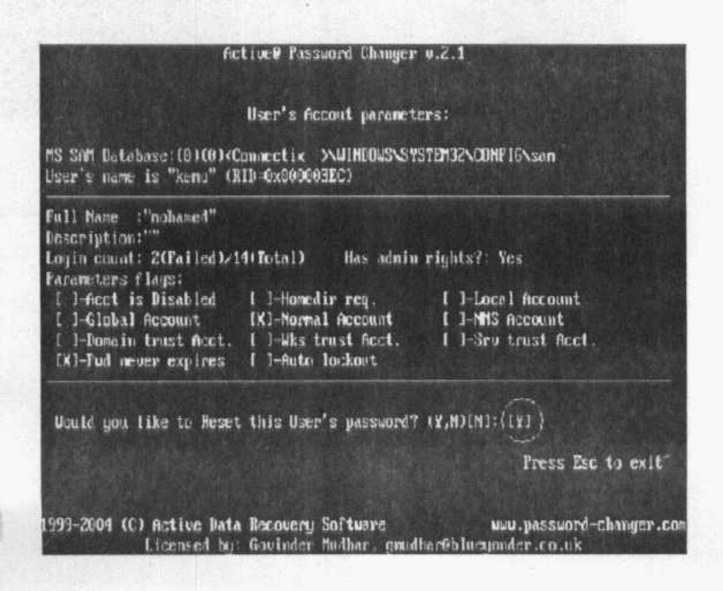
يطلب منك البرنامج فى الشاشة السابقة أن تقوم بضغط Enter لتظهـر الشاشة التالية:



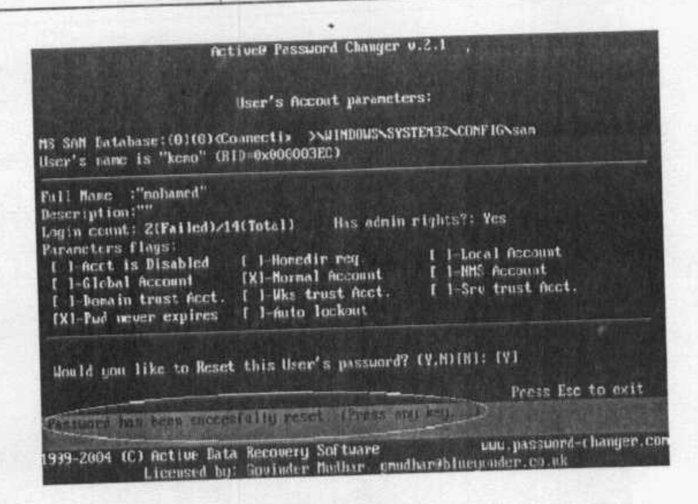
يظهر لك البرنامج من خلال الشاشة السابقة مسار الملف الذى يحتـوى على كلمات المرور بعد أن تعرف عليه ويطلب منك أن تقوم بـضغط مفتاح Enter لتظهر لك الشاشة التالية :



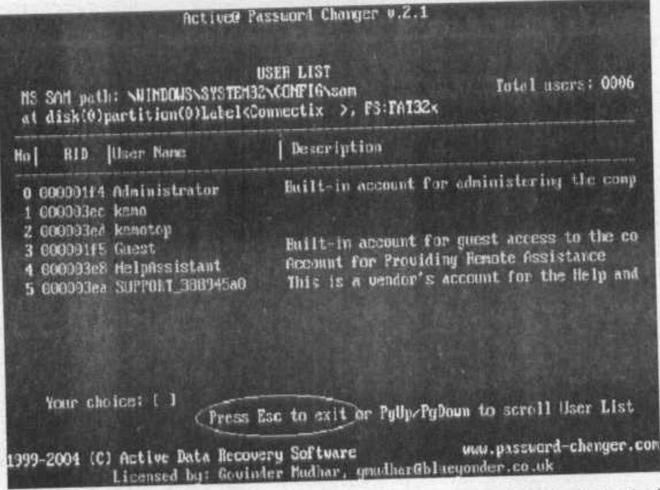
يظهر لك البرنامج فى الشاشة السابقة أسماء المستخدمين داخل الويندوز ومن بينهم حساب Administrator المشار إليه بـــالرقم (0) ويطلـــب منك تحديد المستخدم الذى تريد حذف كلمة المرور الخاصة بـــه وبعـــد إدخال رقم المستخدم الذى تريده كما هو موضح لك والـــضغط Enter تظهر لك الشاشة التالية :



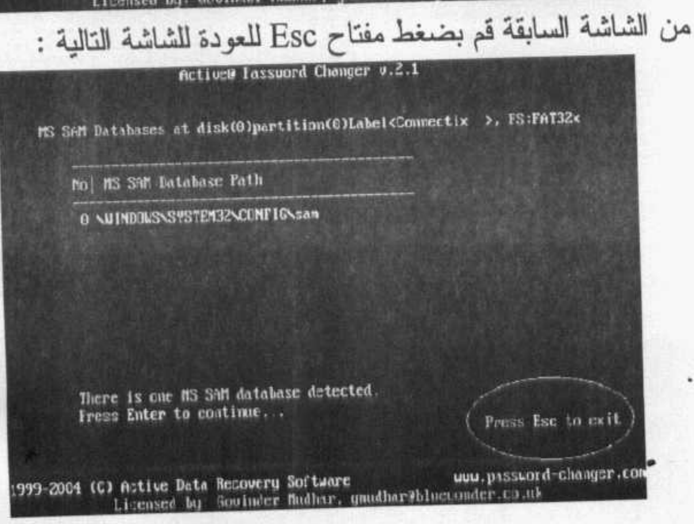
يسألك البرنامج من خلال الشاشة السابقة إذا كنت تريد بالفعـــل حـــذف كلمة المرور بهذا المستخدم فقم بالضغط على الزر (Y) كما مبين لك ثم اضغط Enter لتظهر لك الشاشة التالية :



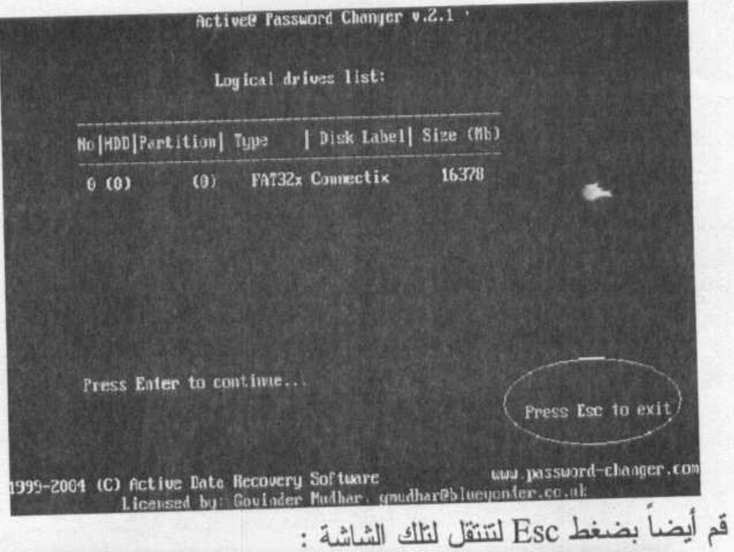
يخبرك البرنامج فى الشاشة السابقة بحذف كلمة المرور ويطلب منك أن تضغط أى مفتاح لتعود للشاشة التالية :



من الشاشة السابقة قم بضغط مفتاح Esc للعودة للشاشة التالية :



من الشاشة السابقة قم أيضاً بضغط مفتاح Esc لتنتقل إلى الشاشة التالية



قم أيضاً بضغط Esc لتنتقل لتلك الشاشة :

```
Active@ Password Changer v.2.1

OPTIONS:

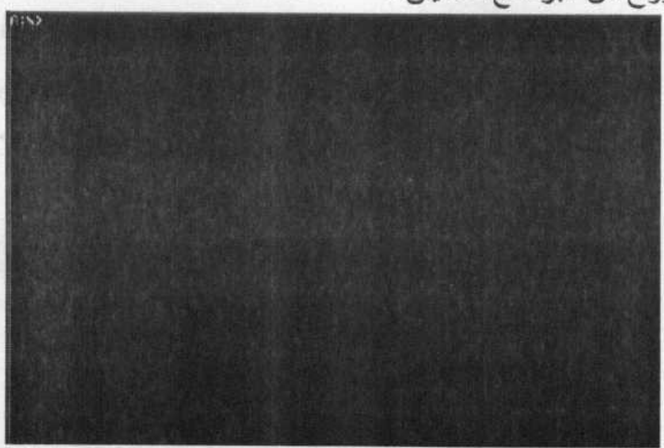
1 Choose Logical Drive
2 Search for MS SAM Database(s) on all hard disks and logical drives
3 Exit

Your choice: [_]

Press Esc to exit

1999-2004 (C) Active Data Recovery Software        www.password-changer.com
Licensed by: Govinder Mudhar, gmudhar@blueyonder.co.uk
```

الشاشة السابقة هى أخر شاشات البرنامج التى تقوم فيها بـضغط Esc للخروج من البرنامج كما يلى :



بعد ذلك قم بإخراج قرص الفلوبى ثم اضـغط مفـاتيح Ctrl + Alt + Delete ليتم إعادة تشغيل الجهاز وستجد أن المستخدم الذى اخترته لـم يعد له كلمة مرور !

أرجو أن تكون تداركت هذه الصدمة وتجاوزتها سريعاً لنتمكن سـوياً من إيجاد حل لهذا المأزق ...

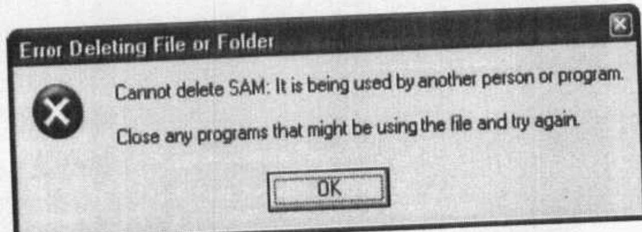
الفكرة التى تقوم عليها هذ البرامج :

فى البداية عليك أن تعرف أين يقوم الويندوز بتخزين كلمات السر ؟

يقوم الويندوز بتخرين كلمات السر فى المسار:

C:\WINDOWS/system32/config

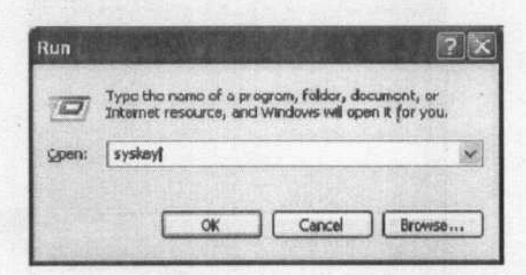
وذلك بعد أن يقوم بتشفيرها وحفظها داخل ملف باسم sam وعليه فإنك إذا قمت بحذف هذا الملف سيصبح جميع المستخدمين ليس لهم كلمة مرور ولكن **لاحظ** أنك لا تستطيع حذف هذا الملف أثناء عمل الويندوز لأنه يكون محمى من نظام التشغيل وعند محاولة حذف هذا الملف ستظهر لك الرسالة التالية :



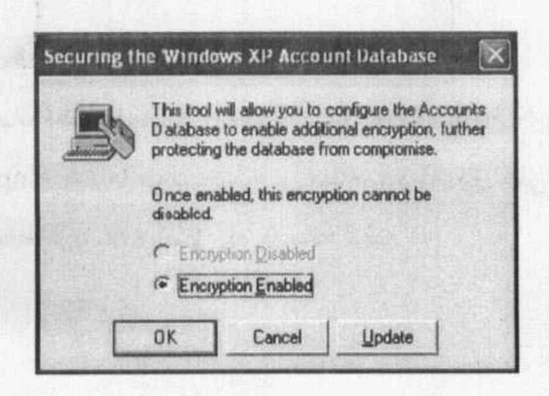
ولذلك يتم إستخدام مثل هذه البرامج التى تعمل بعيداً عن الويندوز لحذفه ... والأن أعتقد أنه يمكنك أن تهدأ من روعك وتطمئن قليلاً بعد أن عرفت هذه المعلومات و بدأت تتضح الصورة لديك فمواجهة المجهول وعدم العلم كثيراً ما يسبب حالة من الخوف والفزع ... ولكن تذكر أننا لم ننتهى بعد ولكننا بمعرفة الداء قد قطعنا نصف طريق للعلاج أم النصف الأخر فيتمثل فى تجهيزك لديسك فلوبى وإتباع الخطوات التالية فهيا بنا ...

إنشاء قرص لإقلاع الويندوز :

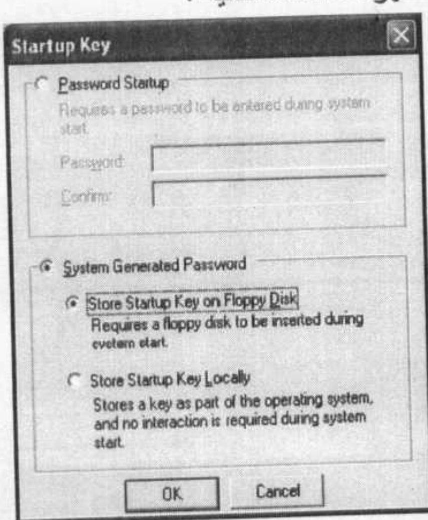
قم بفتح صندوق Run من قائمة start ثم قم بكتابـــة الأمـــر syskey داخله كما يلى :



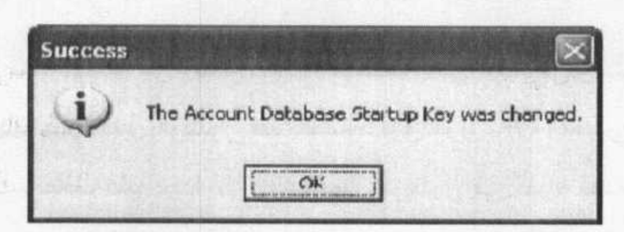
بعد أن تقوم بكتابة هذا قم بالضغط على OK لتظهر لك النافذة التالية :



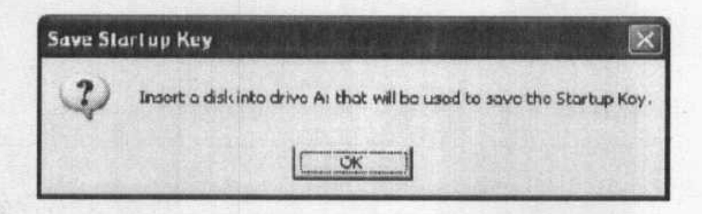
النافذة السابقة هى نافذة البرنامج الذى سنقوم بإستخدامه لنجعل الويندوز يقوم بعمل مفتاح بدء تشغيل Startup Key يكون هو المسئول عن تشغيل الويندوز والدخول إليه ... من النافذة السابقة قم بالضغط على زر Update لتظهر لك النافذة التالية :



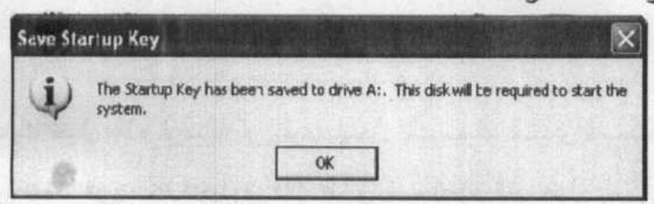
من النافذة السابقة قم بتحديد الإختيار Store Startup Key on Floppy Disk كما هو موضح لتخزين مفتاح بدء التشغيل على فلوبى ديسك ثم أضغط الزر Ok لتظهر لك الرسالة التالية :



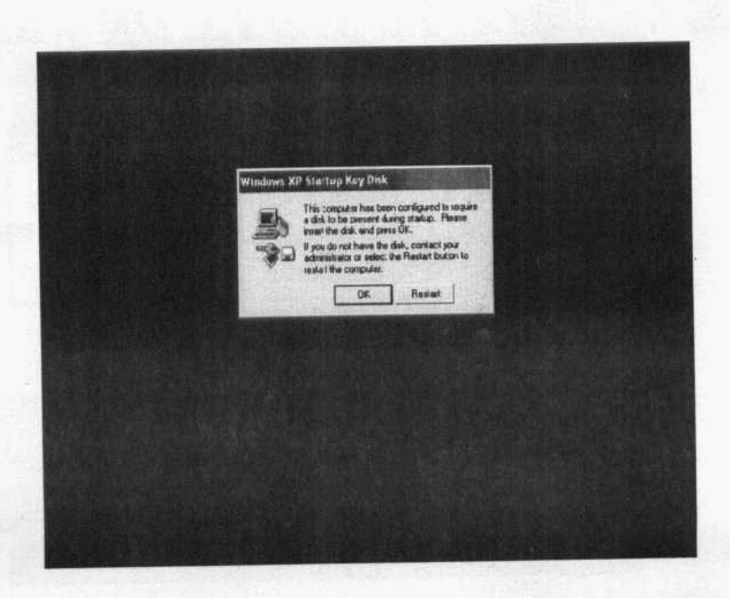
قم بضغط زر OK للرسالة السابقة لتظهر لك الرسالة التالية :



تطلب منك الرسالة السابقة أن تقوم بإدخال ديسك الفلوبى داخل مـــشغل الأقراص المرنة فقم بإدخاله ثم أضغط الزر OK ليبدأ إنشاء الديسك ثم تظهر لك هذه الرسالة.



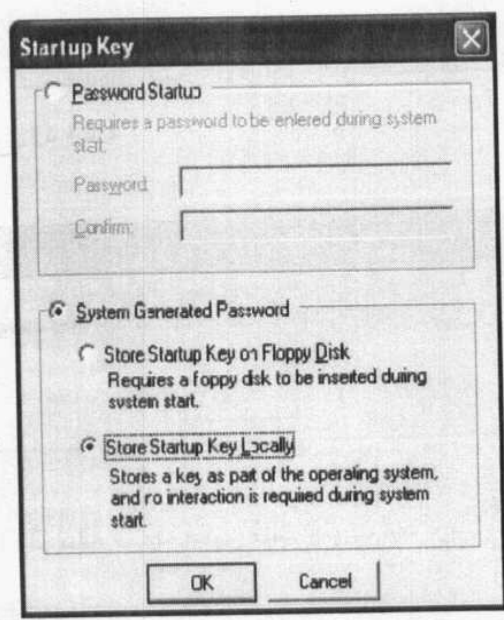
تخبرك الرسالة السابقة بأن مفتاح الأقلاع تم حفظه على الفلــوبى وانـــه سيطلب منك عند تشغيل الويندوز فقم بالضغط فوق الزر OK وأخـــرج هذا الديسك وحافظ عليه جيداً لأن عند تشغيل الويندوز فى المرة القادمة ستظهر لك الرسالة التالية :



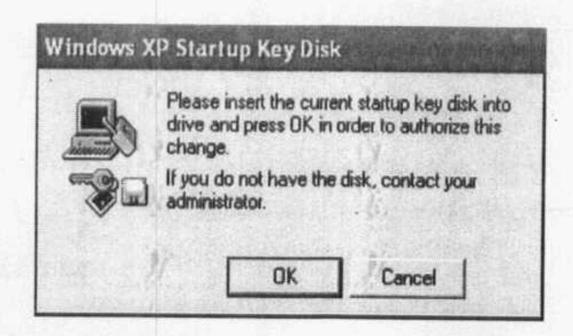
ويجب عليك حيال هذه الرسالة أن تقوم بإدخال الديـــسك الـــذى قمـــت بإنشائه وتضغط الزر OK وبدون ذلك فلـــن تـــستطيع الـــدخول إلـــى الويندوز مرة أخرى لتتساوى فى ذلك مع أى شخص أخر !

مع ملاحظة أن كلمة السر العادية الخاصة بالمستخدم ستظل موجودة أيضاً وتقوم بإدخالها بالطريقة العادية وذلك بعد تخطى مرحلة إدخال الديسك .

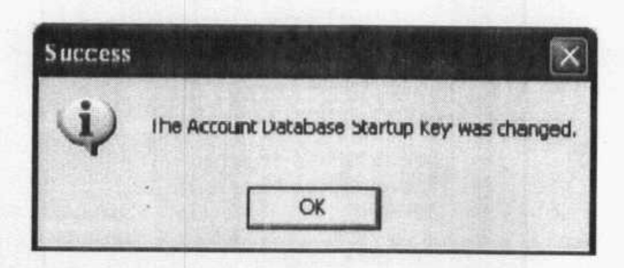
أما فى حالة أردت إلغاء هذا الديسك ستتبع الخطوات الأولى إلى أن تصل إلى هذه النافذة .



فى هذه المرة ومن النافذة السابقة نقوم بتحديد الإختيار Store Startup Key Locally ثم نضغط الزر OK لتظهر لنا الرسالة التالية :



قم الآن بوضع الديسك داخل مشغل الأقراص المرنة ثـم اضـغط OK تظهر بعدها الرسالة التالية :



قم بضغط OK للرسالة السابقة لتكون بذلك إنتهيت مما تريد .

الفصل الخامس

مراقبة الويندوز وتسجيل محاولات الإختراق !

مراقبة الويندوز وتسجيل محاولات الإختراق !

أعتقد أنك الأن وبعد أن تخلصت من هذا الكابوس أن نظرتـك للأمور قد تغيرت وأصبح لزاماً عليك أن تعيد حساباتك مـرة أخـرى وبنظرة أكثر جدية عن ذى قبل .. فالثقة الزائدة والغرور يمكن أن يؤديا بك إلى ما لا يحمد عقباه بل هما أول خطوات فـى طريـق التراخـى والتجربة السابقة خير دليل لك على ذلك وعلى ما يمكن أن تتعرض لـه إذا فكرت بالتهاون فهذا بمثابة جرس إنذار وتحذير لك ورسالة لا بد لنا جميعاً من أن نفهم معانيها ونعيها جيداً ...

وأهم هذه الدروس التى عليك أن تعيها جيداً هو أنه لا يمكنـك أن تطمئن كثيراً لما تعرفه و تركن إليه بل لا بد لك من الحذر فالأمور أصبحت لا تخضع لأى مسلمات والعجلة تدور فى تطور مـذهل فلقـد تعلمنا بالفعل هنا كيف لنا أن نقوم بقطع الطرق وبغلق جميع المنافذ التى ظهرت حتى الأن والتى يمكن أن يتم التسلل من خلالهـا إلـى نظـام التشغيل .

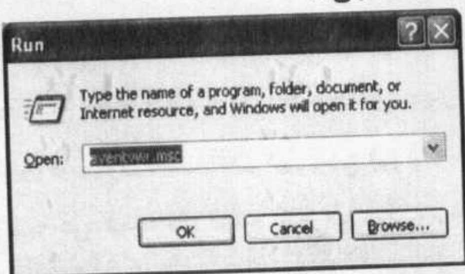
ولكن السؤال الأهم الأن هو كيف تطمئن أنت إلى أنه لن تظهر طريقة أخرى جديدة يتم من خلالها إختراق جميع ما قمت به من طرق حماية وتأمين ؟؟؟ فهذ ما لا يمكن لأحد أن يجيب عليه أو يتنبأ به فقـد تستيقظ فى أحد الأيام لتفاجأ بأن بكمبيوترك والويندوز لـديك قـد تـم

إختراقه والأخطر من ذلك أن تظل معتقداً بأنك فى مأمن وبعيد كل البعد عن أى محاولة (غزو) !!!

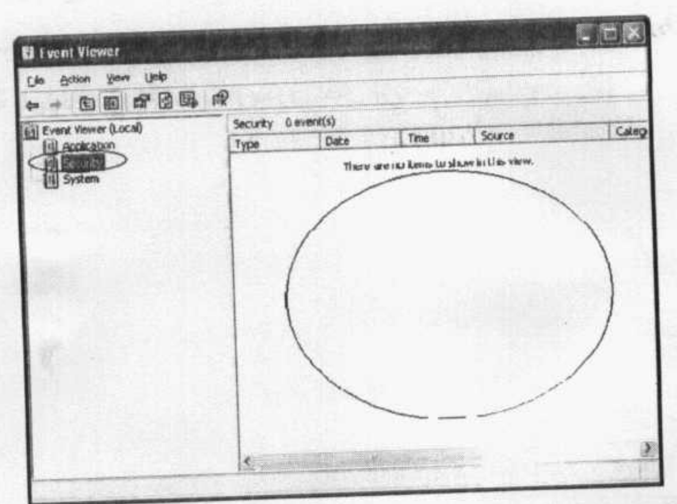
ولكن أعتقد أن من أقل حقوقك أن تطمئن إلى أن هذا اليوم لـــم يأت بعد وأن خصوصياتك ما زالت أمنة ولم يتم إنتهاكها من قبل أحـــد بمعنى أن من حقك أن تعرف هل حاول أحد إختراق جهازك أم لا وإذا كان أحد الأشخاص قد حاول ذلك بالفعل فهل نجح فى ذلك أم فشل فيـــه ؟ وهذا ما سنقوم به فى الخطوات التاليه لنتعرف ونقـــوم بتـــسجيل أى محاولة دخول للجهاز سواء كانت هذه المحاولة شرعية أو غير شرعية وسواء نجحت هذه المحاولة أم فشلت ! فنظام التشغيل ويندوز يحتـــوى بداخله على برنامج يمكنه أن يقدم لنا هذه الخدمة ويقوم لنا بهذه الوظيفة واسم البرنامج المسئول عن ذلك هو Event Viewer فتعـــالى معـــى لنتعرف على طريقة تشغيل هذا البرنامج وكيفية الإســـتفادة مـــن هـــذه الخدمة الجليلة التى يقدمه لنا ويندوز اكس بى .

تشغيل برنامج Event Viewer :

قم بفتح صندوق Run من قائمة start ثم اكتب بداخل الأمـــر eventvwr.msc كما يلى :



بعد كتابة الأمر قم بالضغط على Ok لتظهر لك نافذة البرنـــامج كمــا بالشكل التالى :

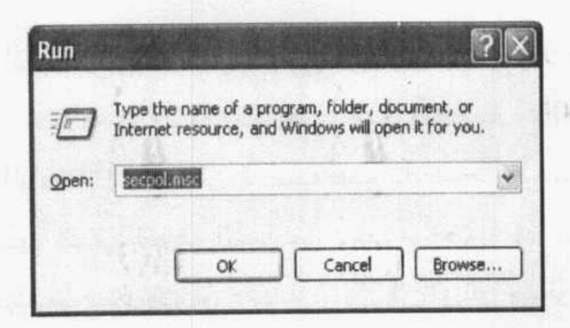


كما ترى بالشكل السابق فالنافذة تنقسم إلى جزئين والجزء الأيسر منها يحتوى على ثلاثة إختيارات ما يهمنا هنا هو الإختيار Security الخاص بنظام بنظام التأمين على الحاسب فقم بالضغط على هذا الإختيار ليظهر لك فى الجانب الأيمن من النافذة ما يحتويه هذا الإختيار وما تم تسجيله من محاولات أو عمليات دخول إلى الويندز ومعلومات عن وقت وتاريخ كل محاولة منها سواء كانت هذه المحاولة ناجحة أو بائت بالفشل ... فماذا ترى ؟ طبعاً لا شيء !!! وذلك لأن هذه الوظيفة فى الوضع الإفتراضى لإعدادات الوينوز تكون معطلة وعليك أن تقوم بتشغيلها بنفسك لكى يمكنك الإستفادة منها وهذا ما سنقوم به فى الخطوات التالية فتابع معى .

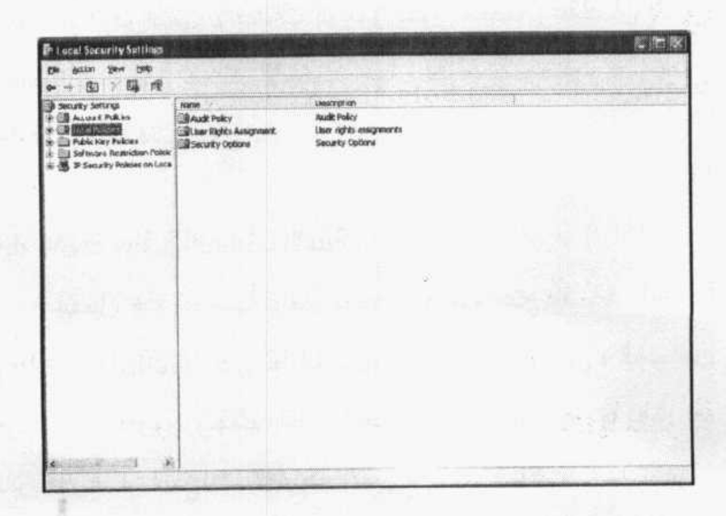
تفعيل خاصية مراقبة التهديدات الأمنية :

لتفعيل هذه الخاصية داخل الويندوز سنقوم بفتح نافذة Local Security Settings التى تعاملنا معها من قبل أثناء الجزء الخاص بتعقيد كلمات المرور وجعلها أكثر فاعلية فعليك أن تقوم بفتحها بالطريقة السابق ذكرها أو اتباع هذه الطريقة الأسرع...

اذهب لقائمة start وقم بفتح صندوق Run لتكتب بداخله الأمر secpol.msc كما بالشكل التالى :

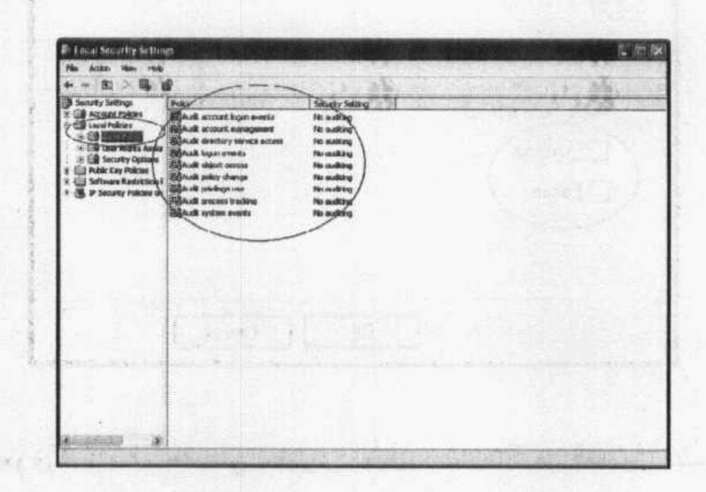


بعد كتابة الأمر السابق والضغط على OK تظهر لك النافذة التالية :

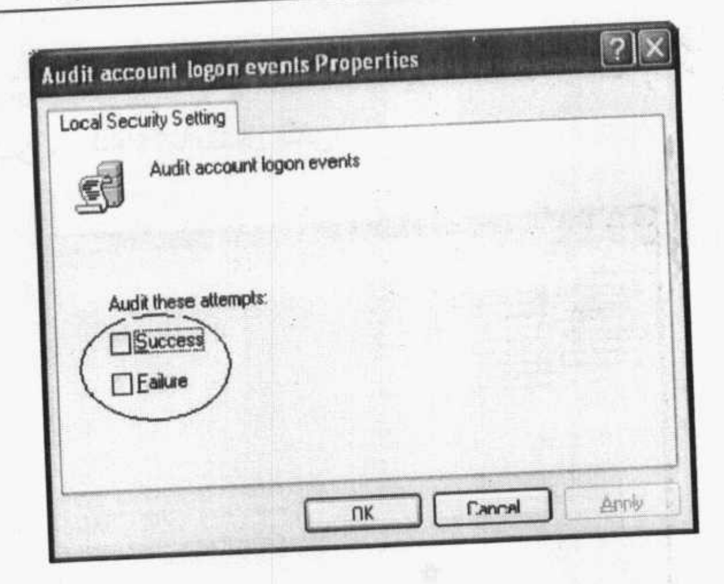


من النافذة السابقة وفى الجزء الأيسر منها سنقوم بالضغط مرتين علـــى المجلد Local Policies ليتفرع منه عدة مجلدات أخـــرى ثـــم نقـــوم

بالوقوف على المجلد Audit Policy لتظهر لنا محتوياته فـــى الجـــزء الأيمن من النافذة كما بالشكل التالى:

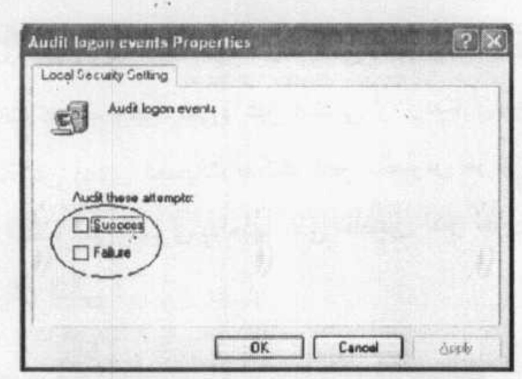


من الجهة اليمنى للنافذة السابقة سنقوم بالتعامل مـــع خاصـــية Audit accound logon events عن طريق الضغط عليها مرتين بالمـــاوس لتظهر لنا النافذة التالية :



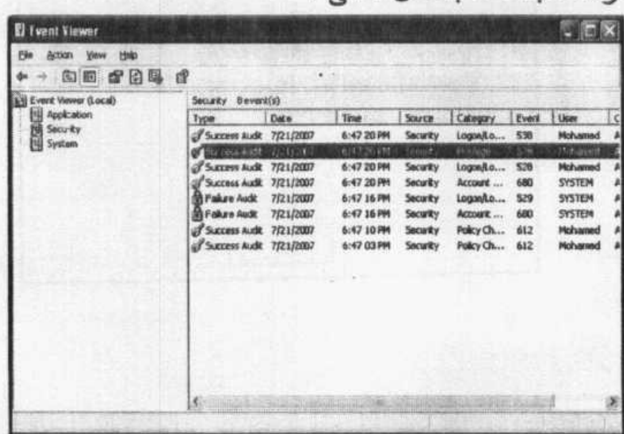
تحتوى النافذة السابقة على إختياران الأول Success هو المسئول عن إظهار العمليات الناجحة للدخول إلى الويندوز أما الثانى فهو Failure وهذا مسئول عن تسجيل المحاولات التى تم الإخفاق فيها فى الدخول للوينوز فقم بالتأشير على الإختيار الخاص بالعملية التى تريد مراقبتها وتسجيل معلومات عنها أو على على الإثنين معاً ثم أضغط الزر OK .

من الجهة اليمنى أيضاً سنقوم بالضغط مرتين على الخاصية Audit logon events لتفتح لنا النافذة التالية :

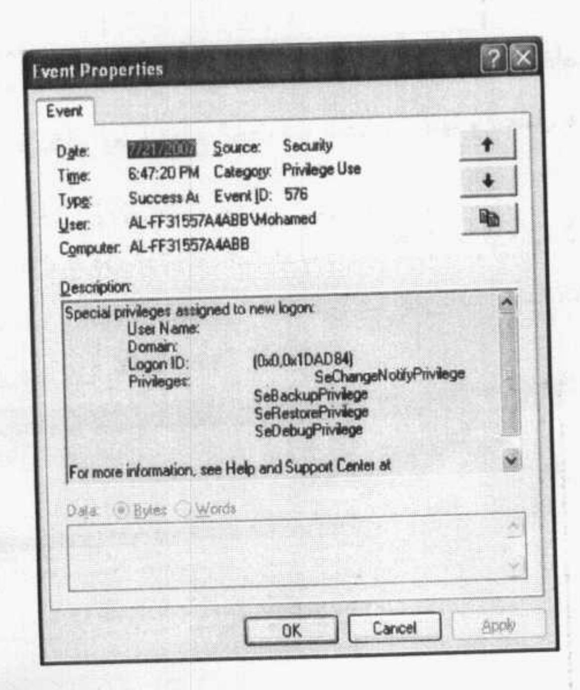


كما ترى فهذه النافذه تحتوى على نفس الإختيارات الموجودة بالخاصية السابقة وعليه فيمكنك أيضاً إتباع الخطوات المذكورة فيها والتعامل معها بنفس الطريقة .

يمكنك الأن الخروج من الويندوز والدخول مرة أخرى ثم الذهاب إلـى برنامج Event Viewer لتجد أن الشكل فى هذه المرة قد أصبح مختلفاً عن المرة السابقة كما بالشكل التالى :



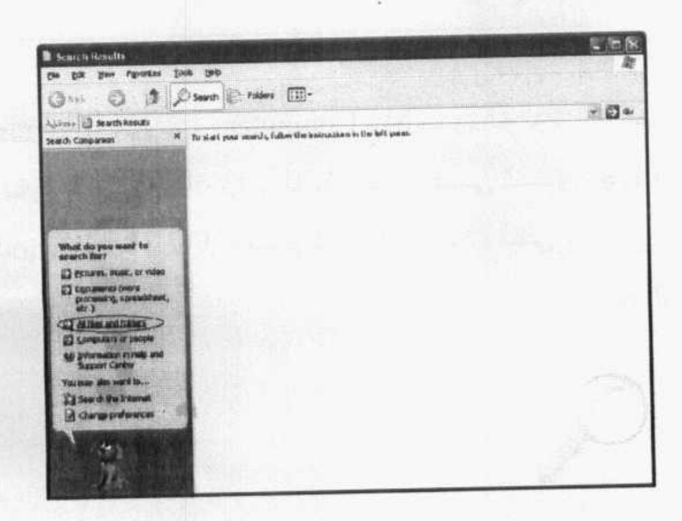
من النافذة السابقة يمكنك مراجعة المحاولات التى تمت للـدخول إلـى الويندوز وإذا لفت نظرك وجود شىء غير طبيعى أو أردت أن تعـرف معومات إضافية عن إحدى العمليات يمكنك النقر بالماوس مرتين عليها لتظهر لك هذه النافذة التى تحتوى بداخلها على تفاصيل أكثر حول تلـك العملية كما بالشكل التالى :



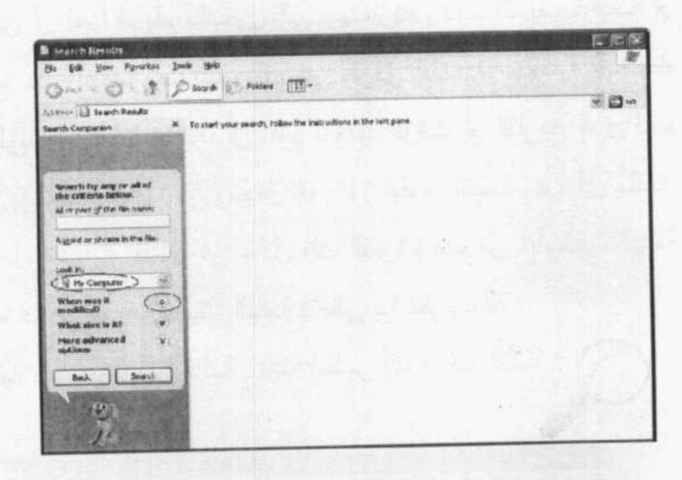
طريقة أخرى للإطمئنان :

يمكنك أيضاً إتباع طريقة أخرى جيدة جـداً وفعالـة إذا أردت التأكد من أن أحداً لم يقم بالدخول إلى جهـازك والعبـث بمـا فيـه أو الإطلاع على أى من ملفاتك وذلك عن طريق إستخدام خاصية البحـث داخل الويندوز فمثلاً يمكنك أن تقوم بتحديد الوقت أو التاريخ الذى لـم تقم فيه بإستخدام الكمبيوتر وتجعل الويندوز يقوم بالبحث عن أى ملفات تم التعامل معها أو فتحها فى خلال تلك الفترة وهذه من الأساليب الهامة والمفيدة لنا فى مراقبة ملفاتنا الهامة فتعالى بنا لنقوم بذلك .

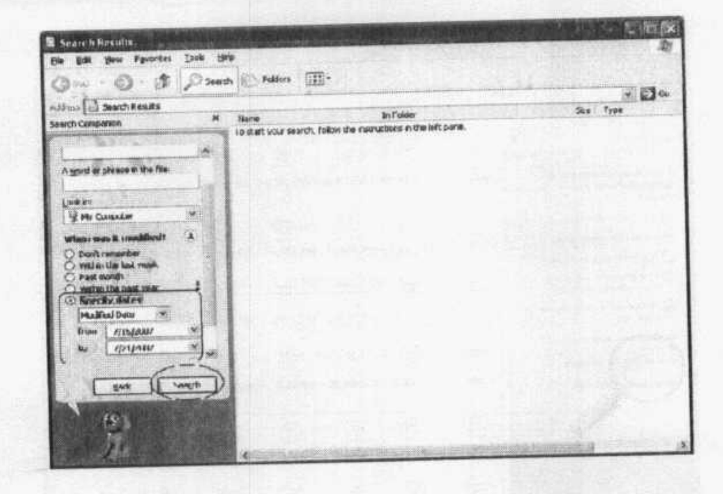
قم بإختيار Search من قائمة start لتظهر لك النافذة التالية :



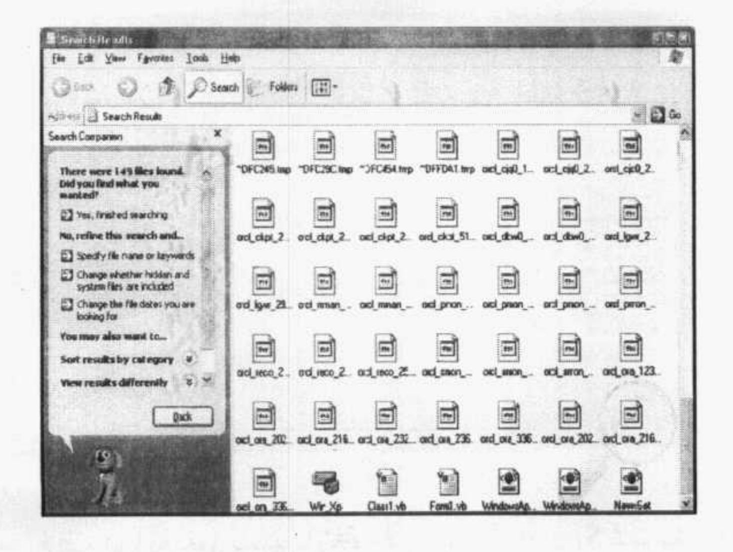
من النافذة السابقة قم بالضغط على All files and folders كما موضح لتظهر لك النافذة التالية :



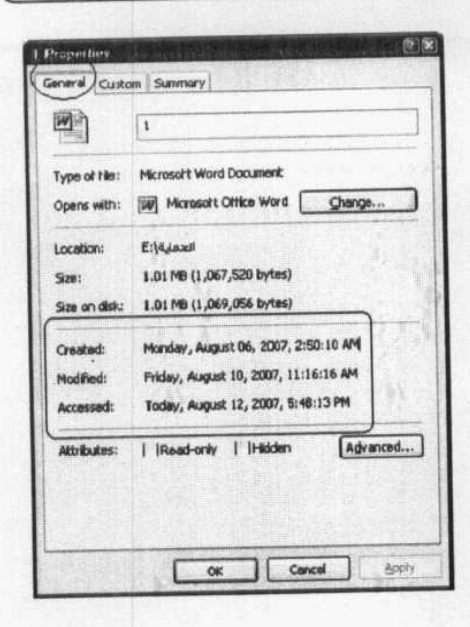
من النافذة السابقة قم بإختيار My Computer من الجزء الخاص بتحديد مكان البحث Look in ثم قم بالضغط على السهم بجوار When was it modified لتصبح النافذة كما بالشكل التالى :



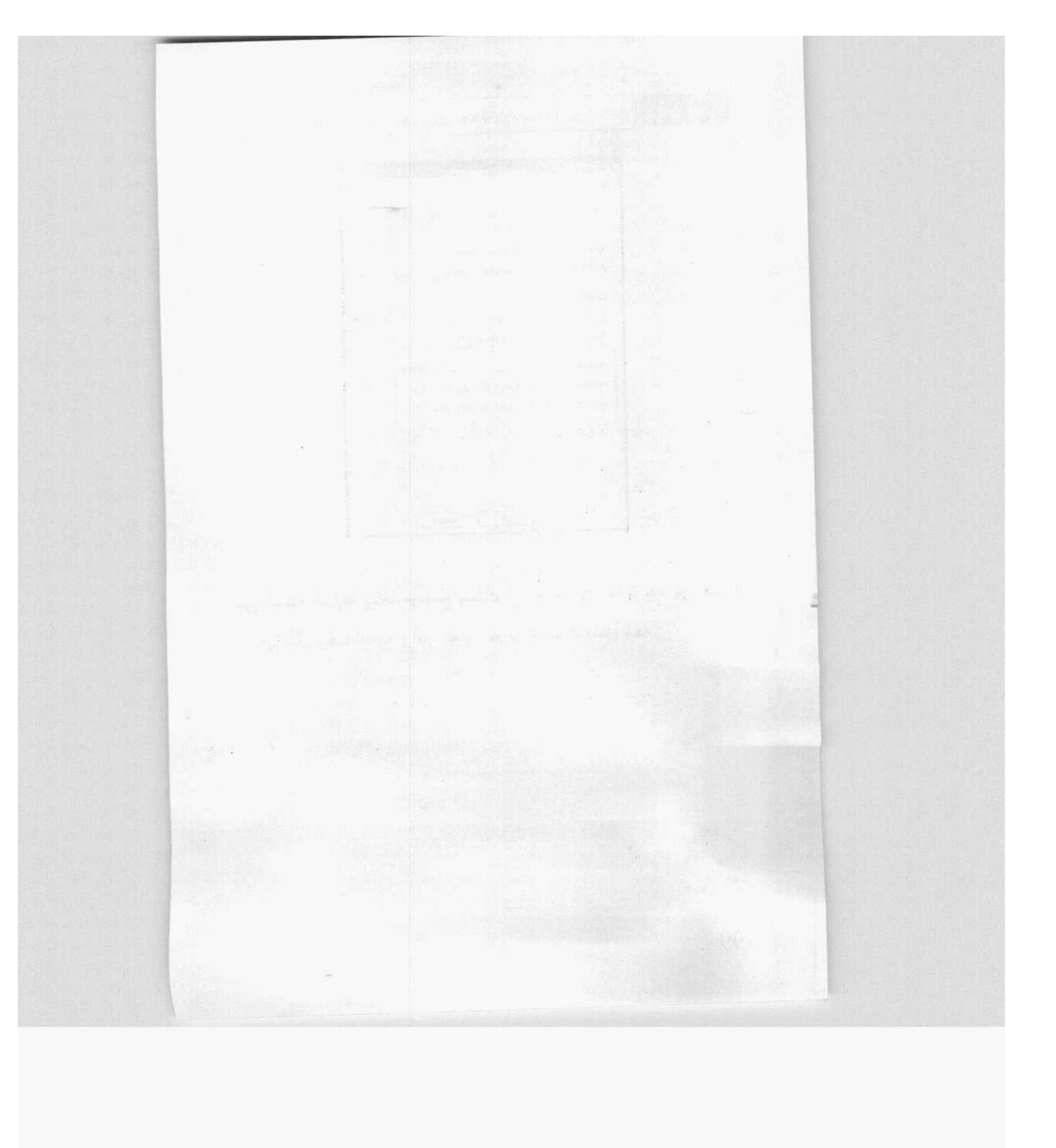
من النافذة السابقة نقوم بتحديد الإختيار Specify dates ثم نختار Modified Date ومن أمام from نقوم بتحديد التاريخ الذى نريد أن يتم البحث إبتدائاً منه ومن أمام to نقوم بتحديد التاريخ الذى ينتهى البحث عنده ثم نضغط بعد ذلك على الزر Sarch ليتم البحث عن أى ملفات تم التعامل معها فى خلال تلك الفترة وإظهار النتائج فى الجهة اليمنى من النافذة كما بالشكل التالى .



لاحظ أنه حتى بدون إجرائك لعملية البحث هذه يمكنك فى أن تقوم بنقـر زر الماوس الأيمن فوق أى ملف لتظهر لك قائمة مختصرة اختر منهـا Properties لتظهر لك النافذة التالية :



من النافذة السابقة وكما موضح يمكنك أن تعرف كل ما تريده عن هــذا الملف مثل وقت إنشائه وأخر تعديل تم به أو تم التعامل معه.



الفصل السادس

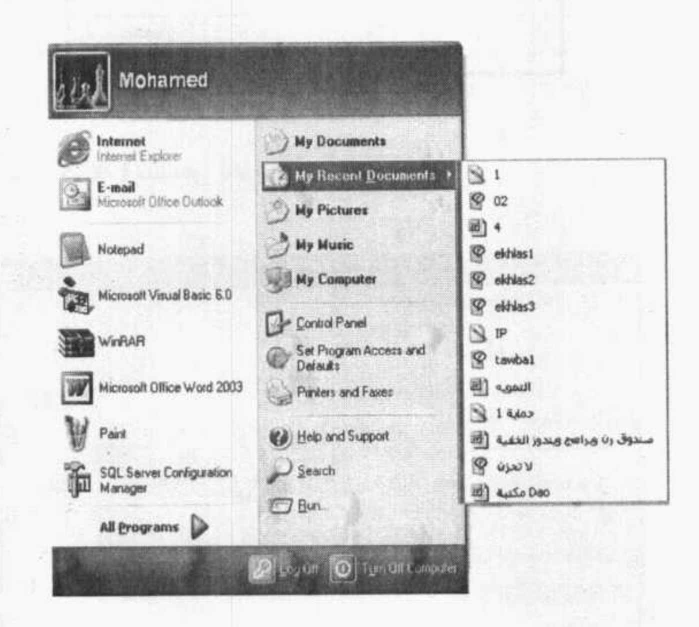
إزالة الآثار

إزالة الآثار

فى الحقيقة ليس معنى ما قمنا به فـى الفـصل الـسابق هـو الإستسلام أو الخضوع فى إنتظار المجهول أو مجرد تسجيل لمحاولات أشخاص غرباء يحاولون التسلل إلى داخل الحاسـب بطريقـة مـا أو بأخرى لنرى ما ستسفر عنه تلك المحاولات ومتى سيتمكن أحدهم مـن الوصول لهدفه ! لا فليس هذا هو المقصود بل هو مجرد بدايـة لخطـة نستكملها فى هذا الفصل وتنتهى مع أخر ورقة بالكتاب وهـذه الخطـة تقوم على إستغلال كل ما هو ممكن ومتاح من أدوات يمكن أن تـشكل لنا درعاً فى مواجهة هؤلاء الأغراب وسنستخدم فى ذلك جميع الطرق المتعارف عليها جنباً إلى جنب مع غيرها من الأفكار والحيل المبتكـرة لنحصل فى النهاية على سد منيع نستطيع من خلاله أن نواجه ونتصدى إلى أى محاولة عدوان يمكن أن نتعرض لها.. أما فـى هـذا الفـصل فسنقوم بتنفيذ أحد أفرع هذه الخطة وهو محو الأثار التـى يمكـن لأى شخص يدخل إلى الجهاز أن يتعقبها ومن خلالها يمكنه الإطلاع على ما نقوم به من عمل وبالتالى نسهل له الوصول إلى أشياء هامـة ببـساطة ودون مجهود وتذكر جيداً أنك إذا تغاطيت عن أحد تلك الأشـياء التـى نقوم بها فى أى جزء من الكتاب فإن ذلك بمثابة تنازل منك عن بعـض درجات التأمين والحماية داخل جهازك !.

قائمة المستندات الأخيرة :

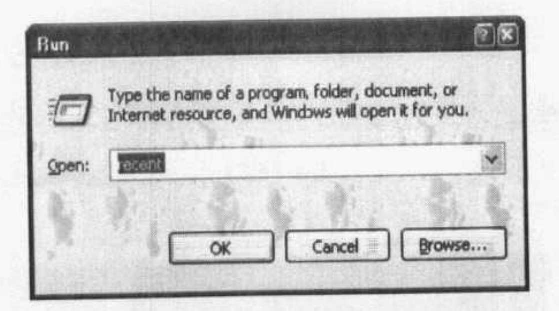
تعود أهمية هذه القائمة لكونها تحتوى أخر مجموعة من الملفات تم التعامل معها كما يتضح لك من الشكل التالى :



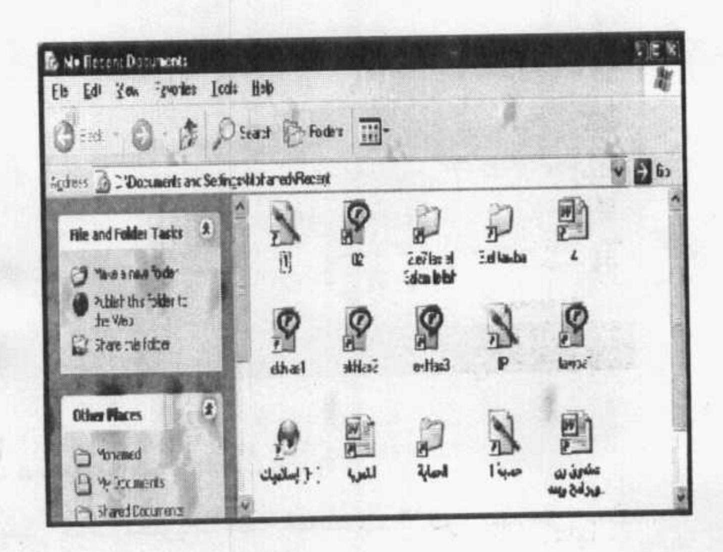
حذف محتويات قائمة المستندات الأخيرة :

يمكن حذف محتويات قائمة المستندات الأخيرة بعدة طرق منها .

1- قم بفتح صندوق Run من قائمة start ثم اكتب داخله recent كما بالشكل التالى :

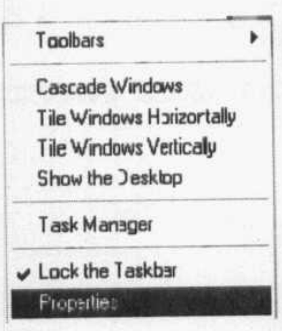


وبعد نقر زر Ok ستظهر لك النافذة التالية :

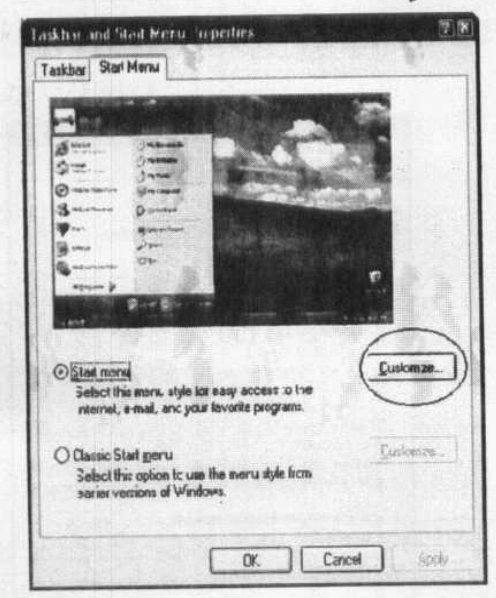


قم بحذف محتويات النافذة السابقة للتخلص من محتويات القائمة .

2- قم بضغط زر الماوس الأيمن فوق شريط المهام لتظهر لك قائمة مختصرة اختر منها Properties كما يلى :



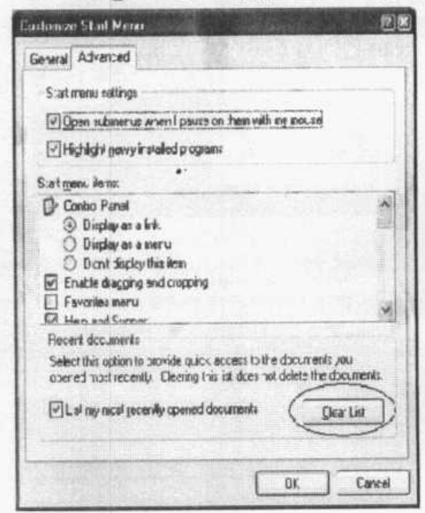
تظهر لك النافذة التالية :



من النافذة السابقة قم بضغط زر Customize لتظهر لك النافذة التالية:



من النافذة السابقة قم بضغط تبويب Advanced المشار إليــه بالــشكل السابق لتتبدل محتويات النافذة إلى الشكل التالى :



من النافذة السابقة قم بضغط زر Clear List كما هو موضح لــك ثــم اضغط زر OK لتكون بذلك قمت بحذف محتويات قائمــة المــستندات الأخيرة كما وإذا عدت لها ستجدها كما بالشكل التالى :

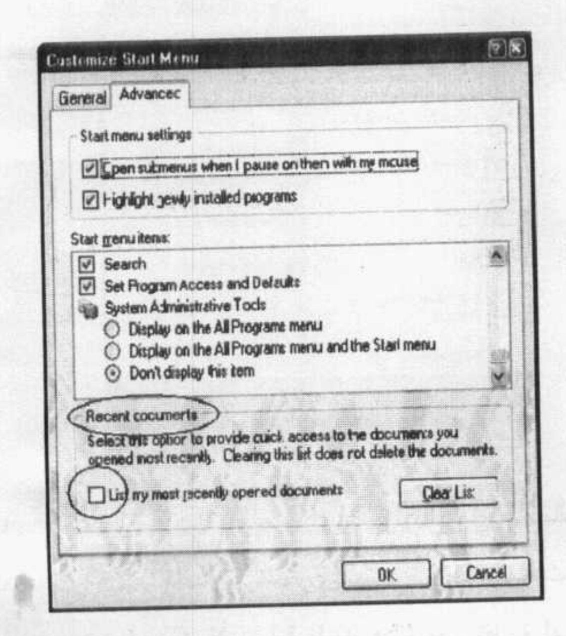


كما ترى فقد أصبحت محتويات القائمة فارغة ولكنك إذا قمت بالتعامــل مع أى ملفات ثم ذهبت للقائمة مرة أخرى ستجد أن هذه الملفات ضيفت إلى القائمة من جديد ! وذلك لأن ما قمنا به هو مجرد تفريغ لمحتوياتها

فقط ولكن يمكنك أن تقوم بمنع إضافة أى ملفات إلى هذه القائمـــة مـــرة أخرى بإتباع عدة طرق كما يلى:

الطريقة الأولى :

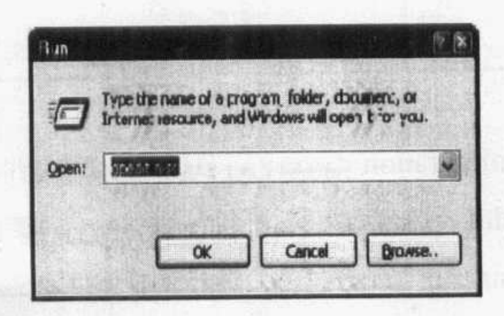
سنعود إلى نافذة Customiz Start Menu التى تعاملنا سابقا لأفـــراغ محتويات القائمة كما بالشكل التالى :



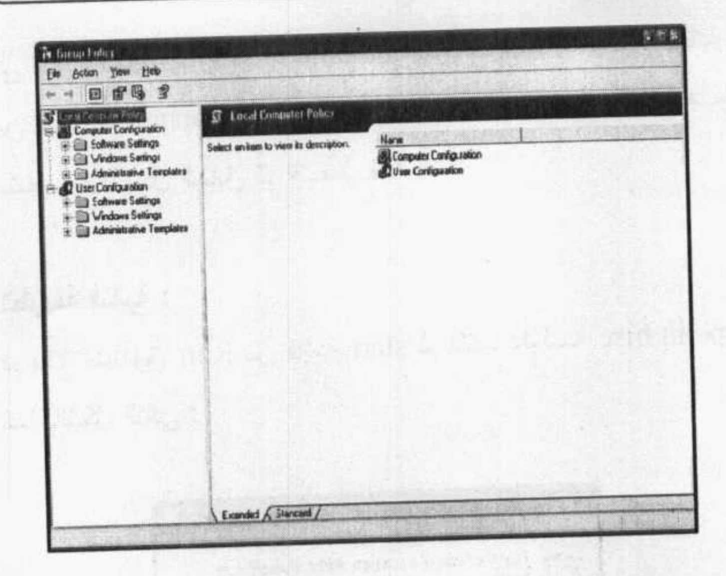
فى النافذة السابقة ومن الجزء Recent documents قم بإلغاء الإختيار من أمام List my most recently opened documents كما هـــو مشار إليه بالشكل السابق ثم اضغط Ok .

الطريقة الثانية :

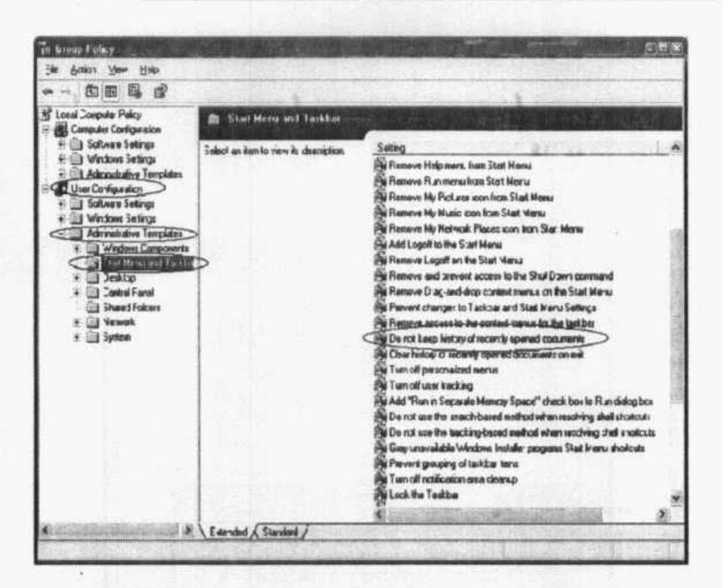
قم بفتح صندوق Run من قائمة start ثم اكتب داخلـــه gpedit.msc كما بالشكل التالى :



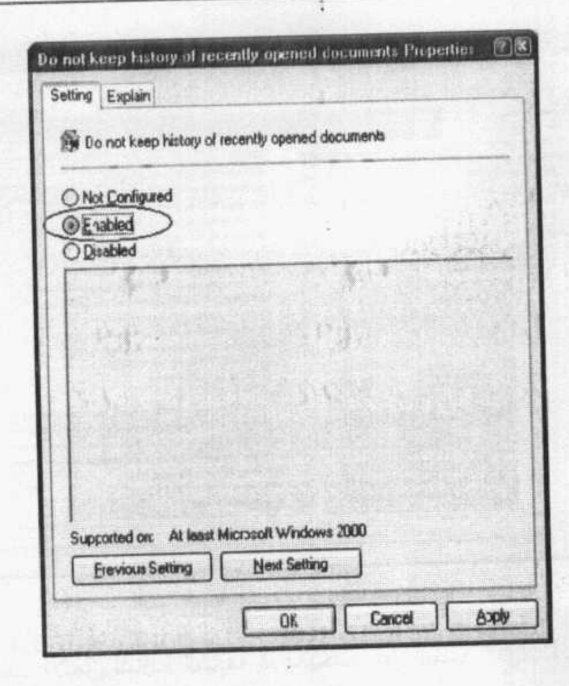
بعد كتابة الأمر انقر الزر OK لتفتح لك نافذة برنامج Group Policy كما بالشكل التالى :



من الجانب الأيسر للنافذة السابقة ومن تحت User Configuration قم بالنقر مرتين فوق المجلد Administrative Templates ليتفرع منه عدة مجلدات أخرى قم بالنقر منها فوق مجلد Start Menu and Taskbar ليظهر لك محتوياته بالجانب الأيمن من النافذة كما يلي :



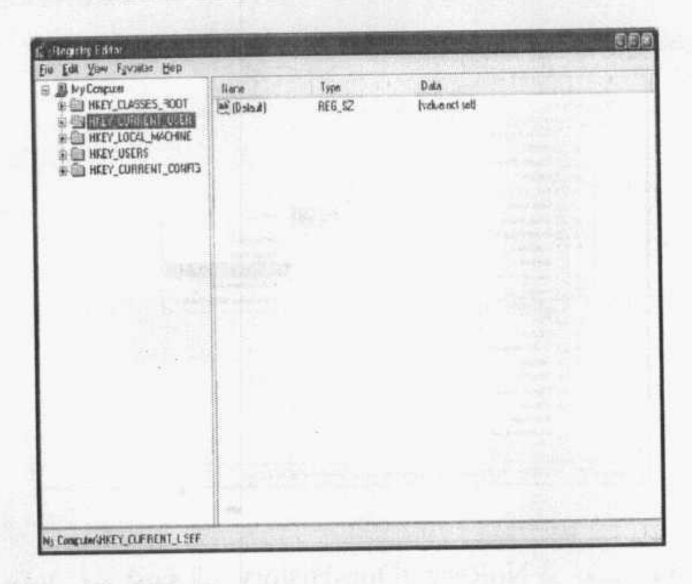
من الجانب الأيمن للنافذة السابقة قم بالبحث عن البنـــد Do not keep history of recently opened documents كما موضح ثـــم انقـــر فوقه مرتين بالماوس لتظهر لك النافذة التالية :



من النافذة السابقة قم بإختيار Enabled كما موضح لك ثم اضغط Ok .

الطريقة الثالثة :

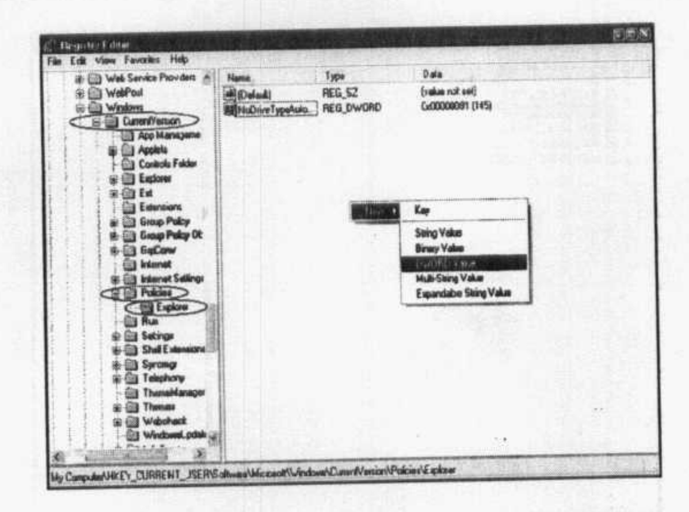
قم بفتح صندوق Run من قائمة start ثم اكتـــب داخلـــه regedit ثـــم اضغط زر Ok لتفتح لك نافذة محرر السجل كما بالشكل التالى :



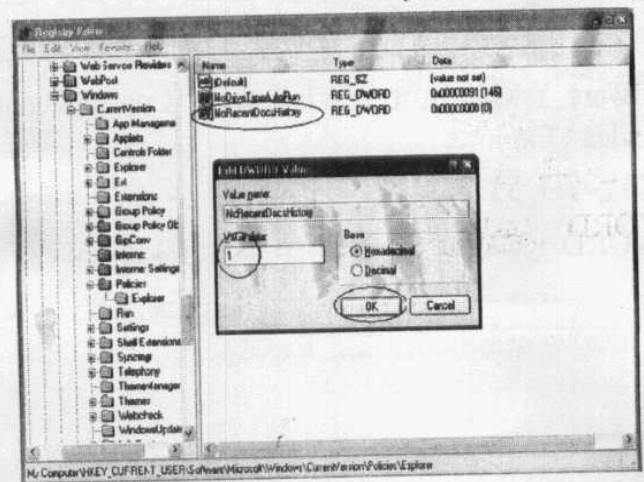
من النافذة السابقة ومن تحـــت HKEY_CURRENT_USER قـــم بالذهاب إلى المسار التالى :

Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer

ثم فى الجانب الأيمن من نافذة محرر السجل قم بنقر زر الماوس الأيمن لتظهر لك قائمة من خيار واحد هو New ومنه قم بإختيار DWORD Value كما بالشكل التالى :



قم بتغيير اسم القيمة الى NoRecentDocsHistory ثم انقــر فوقــه مرتين لتظهر لك النافذة التالية :

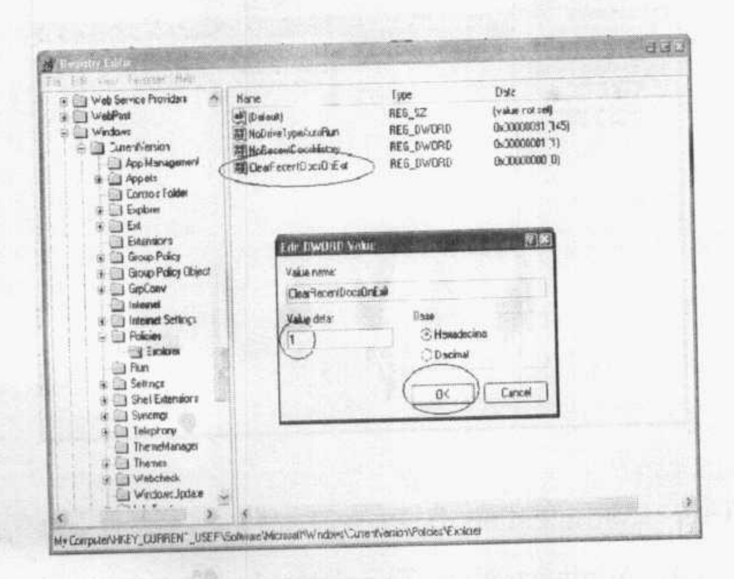


قم بتغيير القيمة إلى واحد (1) ثم اضغط OK كما موضح لك بالشكل السابق ثم أعد تشغيل الجهاز .

حذف قائمة المستندات الأخيرة عند الخروج :

يمكنك كذلك أن تجعل ويندوز يقوم تلقائياً بحذف محتويات قائمة المستندات الأخيرة عند الخروج من خلال محرر السجل كما يلى :

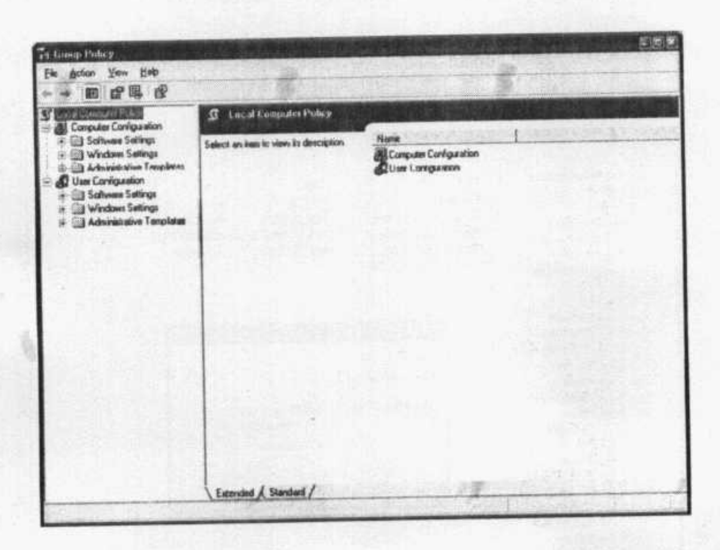
فى نفس المسار السابق قم بإنشاء مفتاح جديد بالاسم ClearRecentDocsOnExit ثم انقر فوقه مرتين لتظهر لك النافذة التالية :



قم بتغيير القيمة إلى واحد (1) ثم اضغط OK كما موضح لك بالـشكل السابق ثم أعد تشغيل الجهاز .

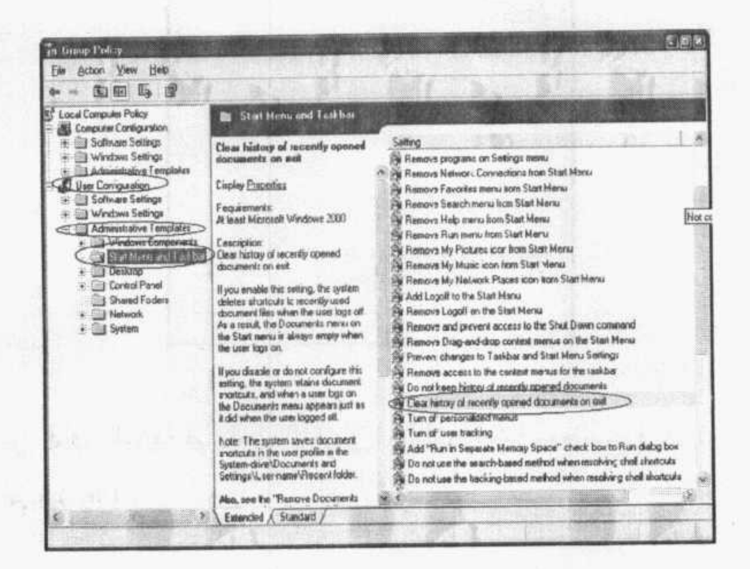
يمكنك أيضاً أن تجعل ويندوز يقوم تلقائياً بحذف محتويات القائمة عنـد الخروج بطريق أخرى كما بالخطوات التالية :

قم بفتح صندوق Run من قائمة start ثم اكتب داخله gpedit.msc ثم انقر OK لتفتح لك نافذة برنامج Group Policy كما بالشكل التالى :

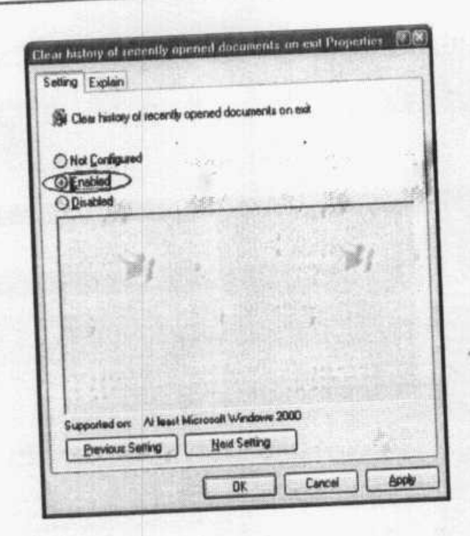


من الجانب الأيسر للنافذة السابقة ومن تحـت User Configuration قم بالنقر مرتين فوق المجلد Administrative Templates ليتفـرع

منه عدة مجلدات أخرى قم بالنقر منها فوق مجلـــد Start Menu and Taskbar ليظهر لك محتوياته بالجانب الأيمن من النافذة كما يلى :



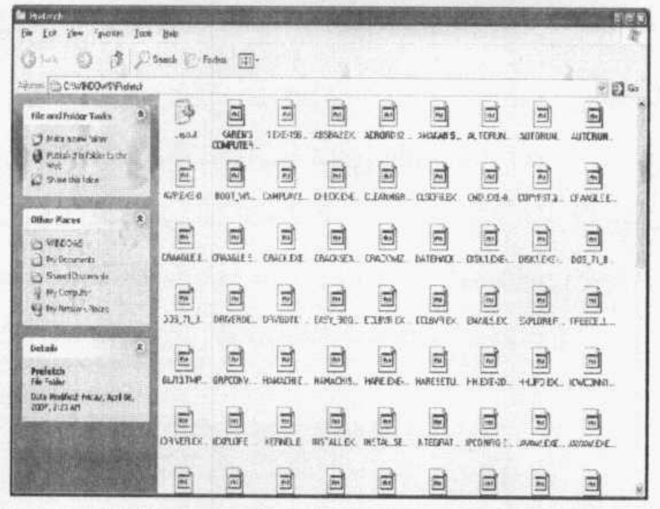
من الجانب الأيمن للنافذة السابقة قم بالبحث عن البنـــد Clear history of recently opend documents on exit كما موضح لك بالـــشكل السابق ثم قم بالنقر فوقه مرتين بالماوس لتظهر لك النافذة التالية بالشكل التالى :



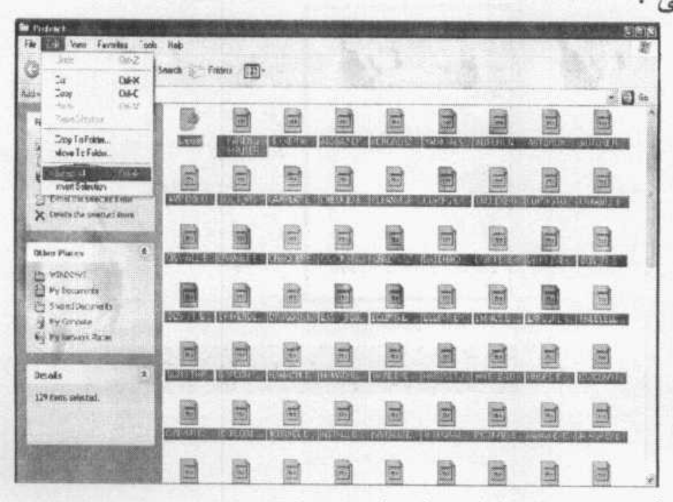
من النافذة السابقة قم بتفعيل الإختيار Enabled كما موضـــح لـــك ثـــم اضغط Ok .

حذف محتويات مجلد prefetch :

هذا المجلد يحوى بداخله معلومات عن الملفات التـــى تتعامـــل معها من قبل نظام التشغيل ومن الأسباب الشائعة لحذف محتويات هـــذا المجلد أنه يقوم بتسريع الويندوز ولكننا سنقوم هنا بحذفه لـــسبب أخـــر أمنى ! ولإظهار محتويات هذا الملف قم بفتح صندوق Run من قائمـــة start ثم اكتب داخله الأمر prefetch ثـــم انقـــر OK لتظهـــر لـــك محتويات هذا المجلد كما بالشكل التالى :



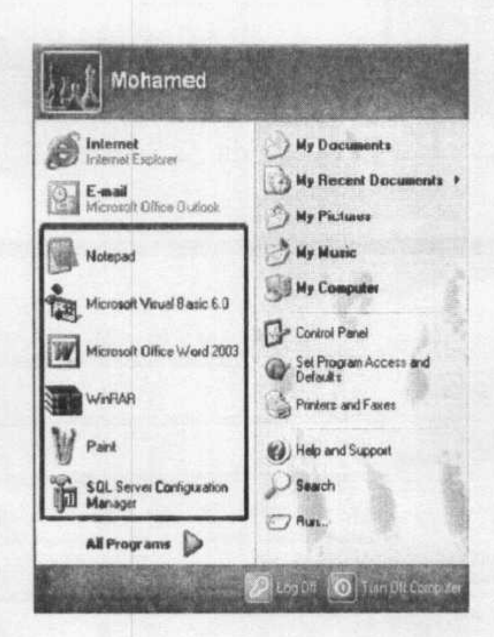
من قائمة بإختيار Select All من Edit لتحديد كل الملفات كما بالشكل التالى :



قم الآن بحذف تلك الملفات لتتخلص منها .

منع تتبع المستخدم :

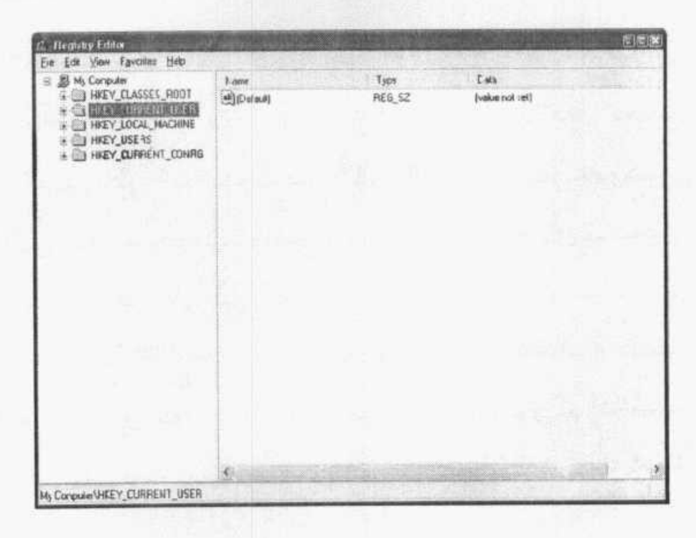
يحتوى الويندوز على أحد الخواص الهامة التى يقوم من خلالها بتسهيل عمل المستخدم وهذه الخاصية تسمى user tracking أو تتبع المستخدم وكما يتضح من اسم هذه الخاصية فإن الويندوز يتعرف من خلالها على ما يتم التعامل معه من قبل المستخدم كالبرامج والشكل التالى مثال على ما يمكن أن تقوم به هذه الوظيفة .



كما يتضح لك بالشكل السابق يقوم الويندوز فى الجهة اليسرى لقائمة start بإظهار أخر مجموعة برامج قام المستخدم بالتعامل معها بغرض التيسير على المستخدم للوصول إلى تلك البرامج بسرعة وكما ترى فإنها وظيفة هامة ومفيدة ولكنها فى نفس الوقت تتيح لأى شخص التعرف بسهولة على أخر البرامج التى قمت بالتعامل معها ولذلك قد تكون مضطراً إلى التضحية بهذه الوظيفة من أجل المحافظة على السرية أو يمكنك أن تقوم بإلغائها قبل الخروج من الويندوز ثم إعادتها مرة أخرى عند العودة وسنتعرف على أكثر من طريقة للقيام بذلك كما يلى .

الطريقة الأولى :

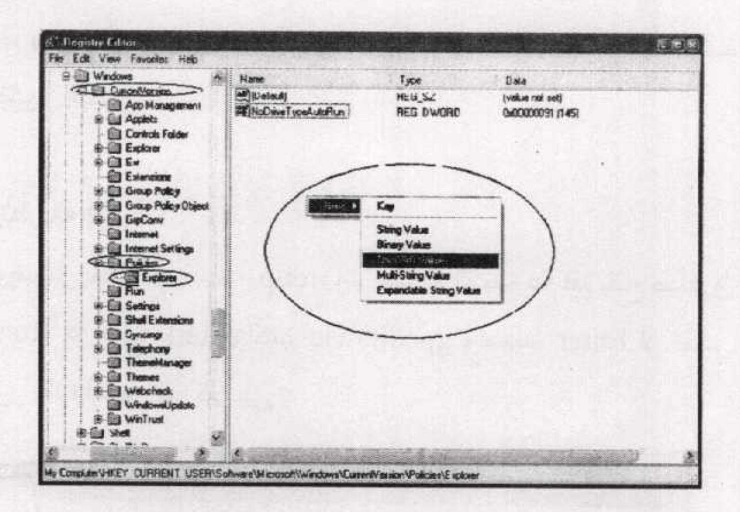
وتتم من خلال محرر السجل فقم بفتحه عن طريقة قائمة start واختر منها Run ثم اكتب regedit واضغط Enter أو انقر زر Ok لتفتح نافذة محرر السجل كما يلى :



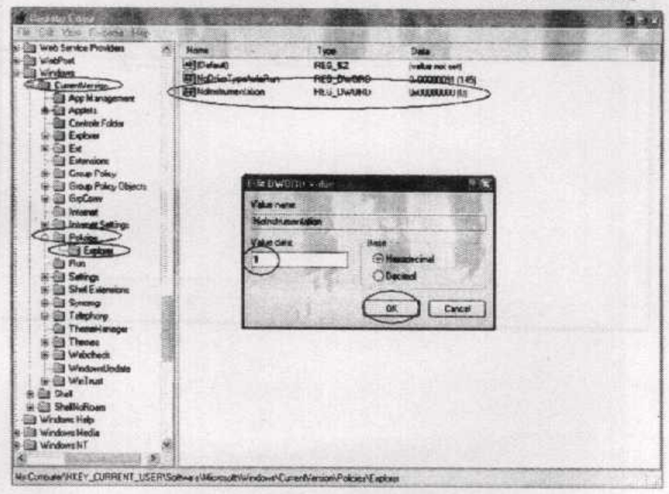
من النافذة السابقة ومن تحـت HKEY_CURRENT_USER قـم بالذهاب إلى المسار التالى :

Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer

ثم فى الجانب الأيمن من نافذة محرر السجل قم بنقر زر الماوس الأيمن لتظهر لك قائمة من خيار واحد هو New ومنه قم بإختيار DWORD Value كما بالشكل التالى :



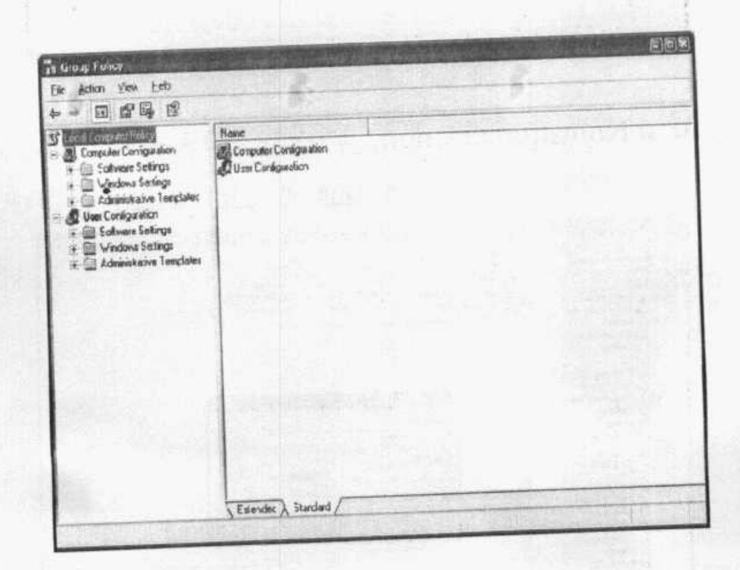
قم بتغيير اسم القيمة الذى أنشأتها إلى NoInstrumentation ثم أنقــر فوقه مرتين بالماوس لتظهر لك النافذة التالية :



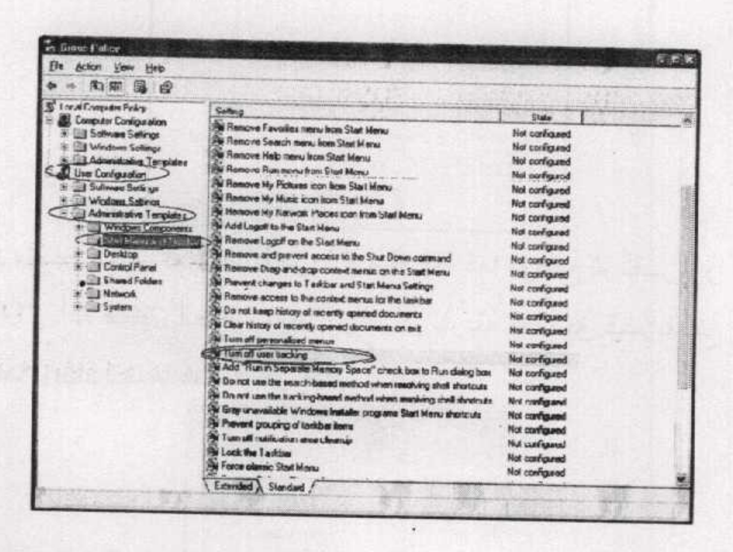
قم بتغيير القيمة إلى واحد (1) ثم اضغط OK كما موضــح ثــم أعــد تشغيل الجهاز .

الطريقة الثانية :

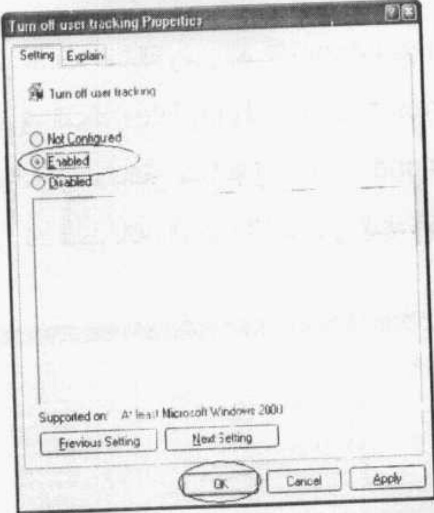
وتتم من خلال Group policy أو سياسة المجموعة فقم بفتح صندوق Run من قائمة start واكتب gpedit.msc واضغط Enter أو انقــر زر Ok لتظهر لك كما يلى :



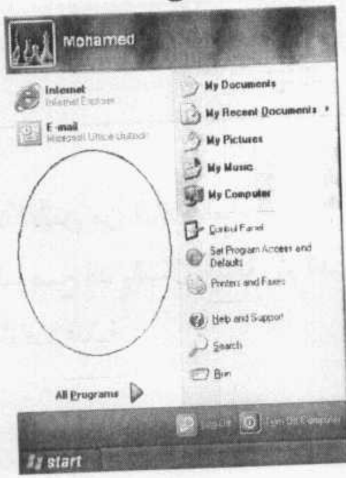
من الجانب الأيسر للنافذة السابقة ومن تحـت User Configuration قم بالنقر مرتين فوق المجلد Administrative Templates ليتفـرع منه عدة مجلدات أخرى قم بالنقر منها فوق مجلـد Start Menu and Taskbar ليظهر لك محتوياته بالجانب الأيمن من النافذة كما يلى :



قم بالبحث فى الجانب الأيمن من النافذة السابقة عـن البنـد Turn off user tracking الموضح لك بالشكل السابق ثم انقـر فوقـه مـرتين بالماوس لتظهر لك النافذة التالية :



قم بتنشيط الخيار Enabled من النافذة السابقة كما موضح ثم أنقــر زر Ok و أعد تشغيل الجهاز. وبعد تنفيذك أى طريقة.مما سبق قــم بفــتح قائمة start لتجدها كما بالشكل التالى .



الفصل السابع

حماية الأقراص

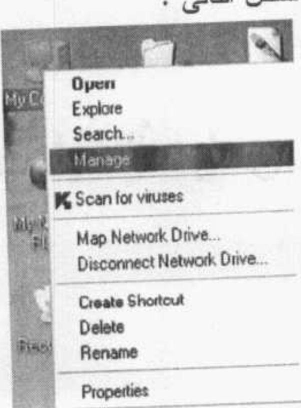
حماية الأقراص

الأقراص الصلبة من أهم الأشياء التى لا بد لنا من محاولة تأمينها وحمايتها بأفضل وأقوى الطرق الممكنة فهى بمثابة الوعاء الذى يحوى بداخله كل شىء من ملفات وغير ذلك وإذا استطعت أن تخفى تلك الأقراص فأنت بذلك تكون قد محوت طريق الوصول إلى أى ملفات بالجهاز ولكن فى كثير من الأحيان لا يصبح ذلك كافياً ! وعليك البحث عن حلول وسبل أخرى أفضل لحمايتها وهذا وذاك هو ما سنتعرف عليه فى هذا الفصل.

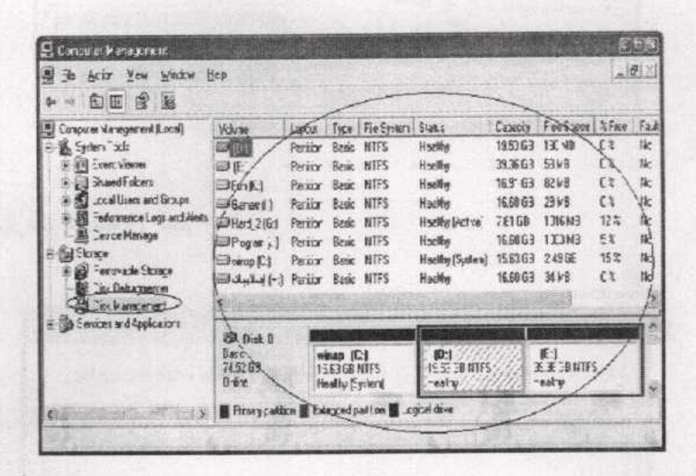
إخفاء محركات الأقراص :

يمكن إخفاء محركات الأقراص بعدة طرق منها ما يلى :

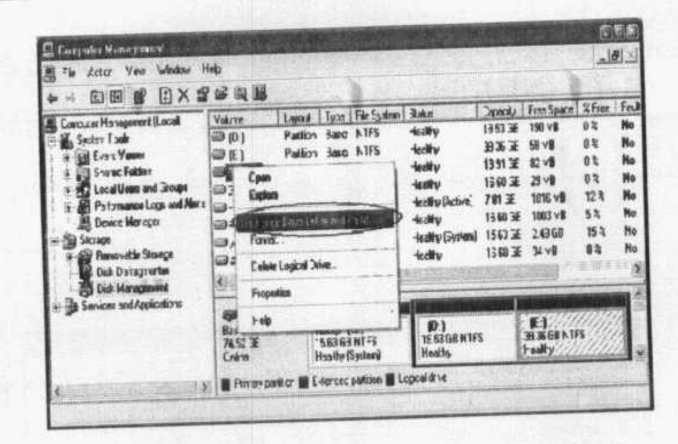
قم بنقر زر الماوس الأيمن فوق رمز My Computer لتظهر لك قائمة مختصرة كما بالشكل التالى :



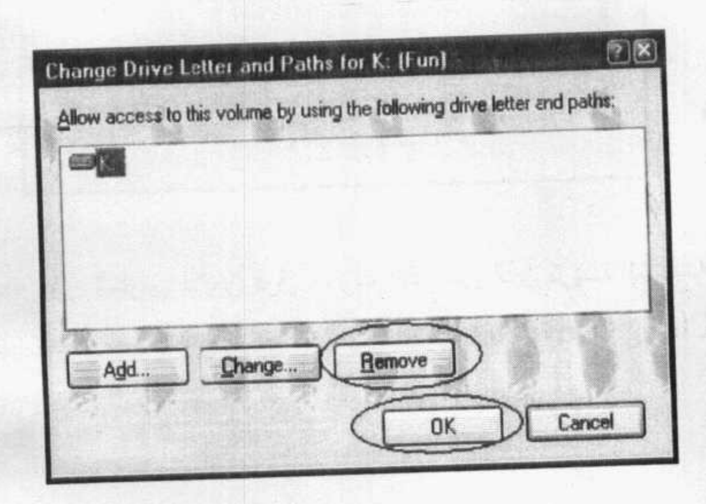
من القائمة السابقة قم بإختيار Manage لتظهر لك نافـــذة Computer Management ثم قم بنقر Computer Management مـــن جهـــة اليسار لتظهر لك فى الجانب الأيمن من النافذة جميع الأقراص الـــصلبة كما بالشكل التالى :



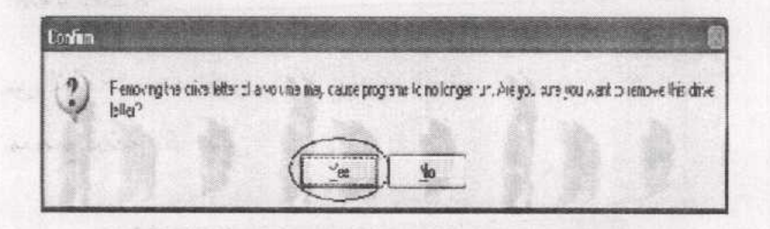
قم بنقر زر الماوس الأيمن فوق محرك الأقراص الذى تريـــد إخفائـــه لتظهر لك قائمة مختصرة اختر منهـــا Change Drive Letter and Paths كما بالشكل التالى :



ليظهرلك صندوق الحوار التالى :

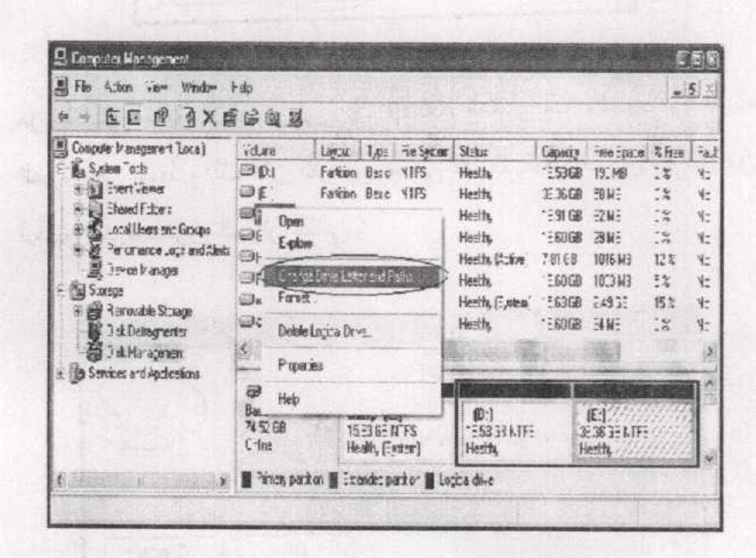


قم بنقر زر Remove ثم انقر Ok لتظهر لك الرسالة التاليه :

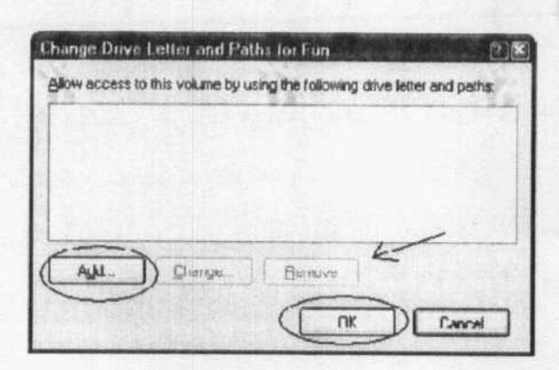


قم بنقر زر Ok لتختفى الرسالة ويختفى معها القرص الذى أخترته ثــم كرر أخر خطوتان مع جميع الأقراص .

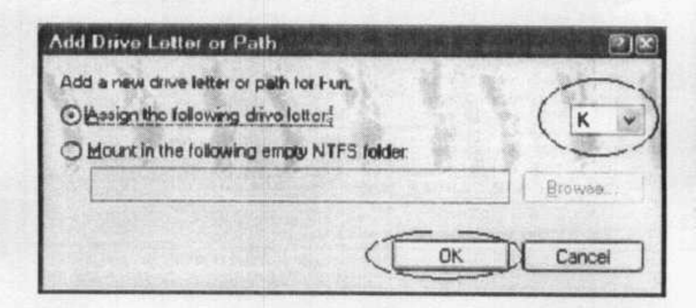
أما إذا أردت إظهارها مرة أخرى فقم بنقر زر الماوس الأيمــن فــوق القرص الذى تريد إظهاره لتظهر لك قائمة مختصرة كما يلى :



من القائمة السابقة اختـــر Change Drive Letter and Paths كمـــا موضح ليظهر لك التالى :



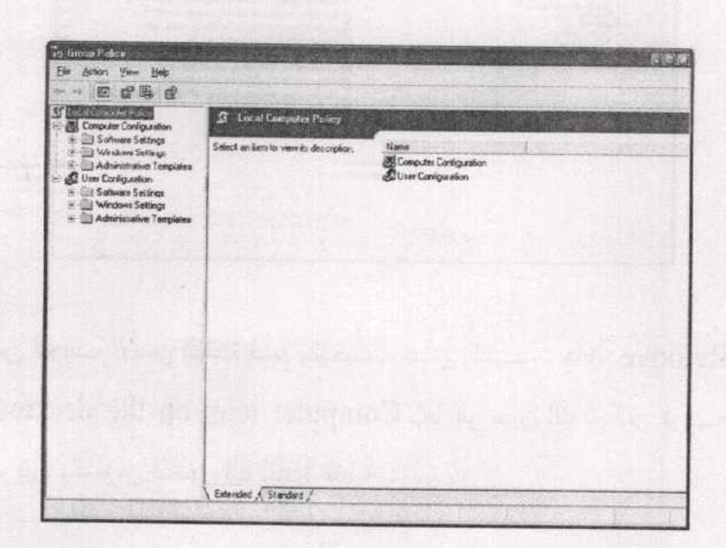
من الشكل السابق لاحظ أن زر Remove المشار إليه بالسهم فى هـــذه المرة غير نشط وذلك لأن القرص مخفى فقم بـــالنقر فـــوق زر Add ليظهر لك صندوق الحوار التالى :



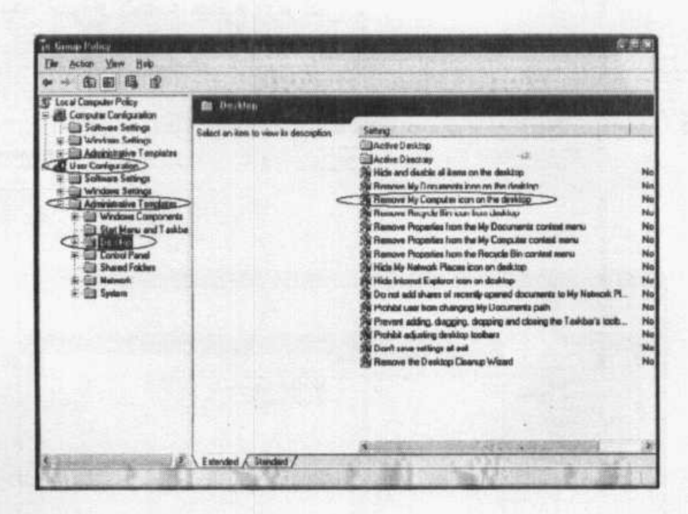
من القائمة المنسدلة الموضحة بالشكل السابق قم بإختيار رمز القــرص المراد إظهاره وستجد أن البرنامج تعرف تلقائياً كما يظهر لك فلا داعى لتغييره ثم اضغط فوق الزر Ok .

طريقة أسرع لإخفاء جميع الأقراص :

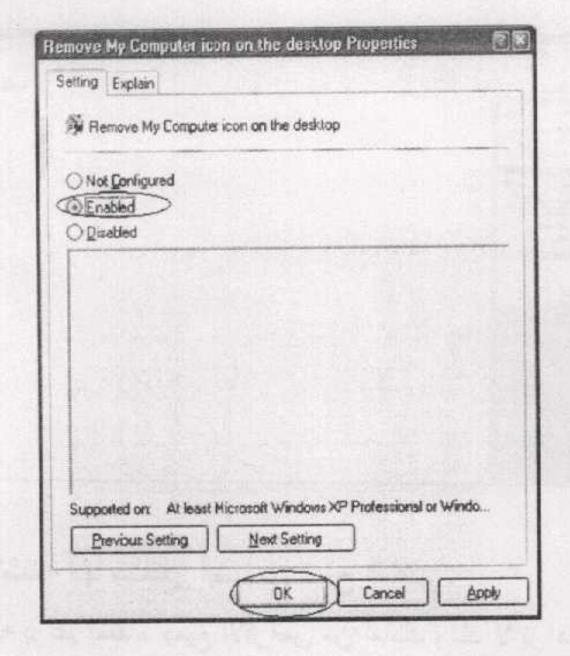
قم بفتح صندوق Run مــن قائمــة start ثــم اكتــب داخلــه gpedit.msc ثم انقر OK لتفتح لك نافذة برنامج Group Policy كما بالشكل التالى :



من الجانب الأيسر للنافذة السابقة ومن تحـــت User Configuration قم بالنقر مرتين فوق المجلد Administrative Templates ليتفـــرع منه عدة مجلدات أخرى قم بالنقر منها فوق مجلد Desktop ليظهر لك محتوياته بالجانب الأيمن من النافذة كما يلي :

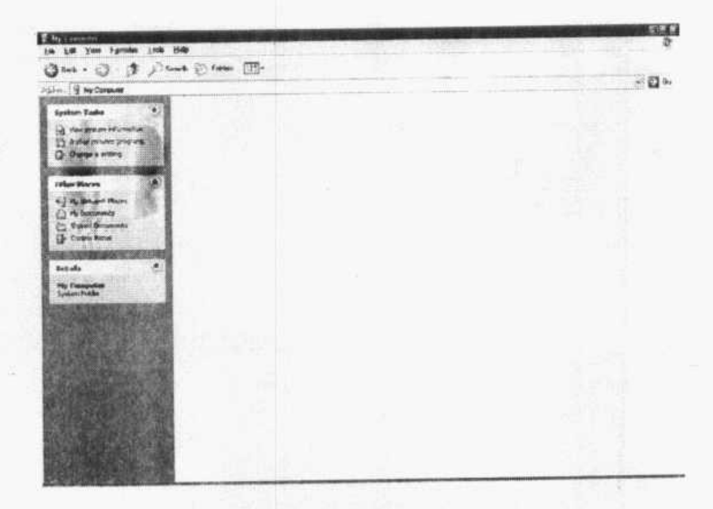


من الجانب الأيمن للنافذة قـــم بالبحـــث عـــن البنـــد Remove My Computer icon on the desktop كما هو مبين لك ثم انقر فوقـــه مرتين بالماوس لتظهر لك لنافذة التالية :



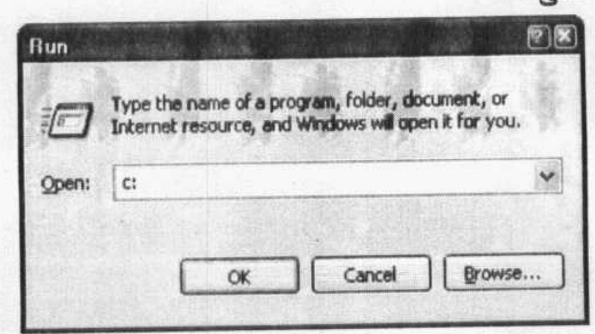
من النافذة السابقة قم بإختيار Enabled ثم نقر Ok .

والأن عند الذهاب إلى نافذة My Computer ستجدها خاوية مـــن أى أقراص كما يلى :



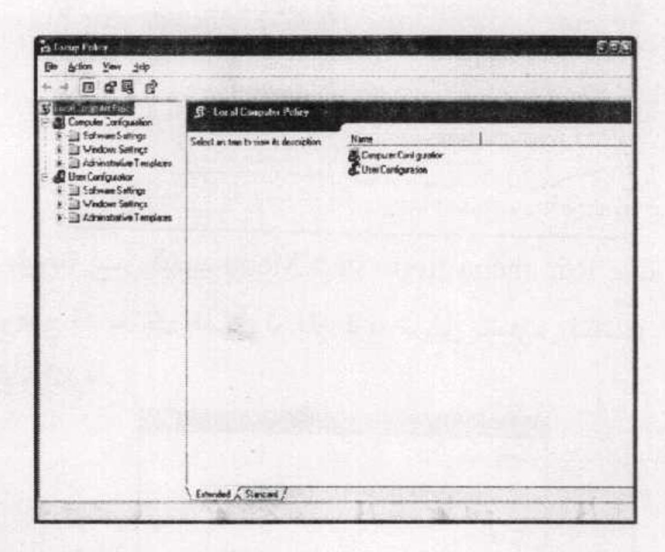
هذا بالإضافة أنها ستختفى أيضاً من سطح المكتب .

لاحظ أنه برغم إختفاء جميع الأقراص من أمامك وأنك لا تراهـا إلا أن ذلك لا يمنع من الوصول لها بسهولة من خلال صندوق Run ثم كتابة رمز محرك القرص الذى تريد الوصول له والنقر فـوق زر Ok كمـا بالشكل التالى :

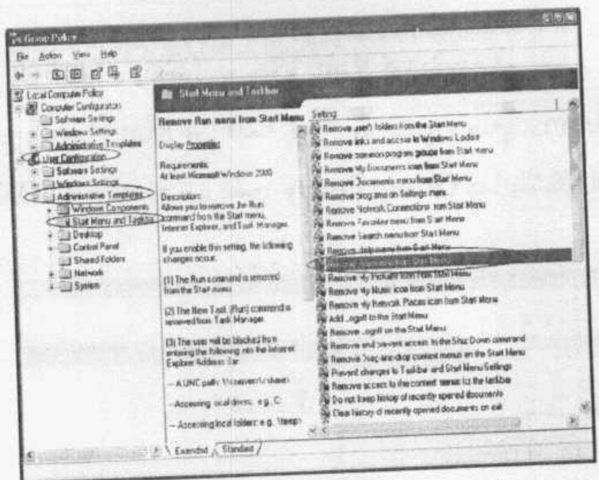


سنقوم الأن بإخفاء وتعطيل صندوق Run كما يلى :

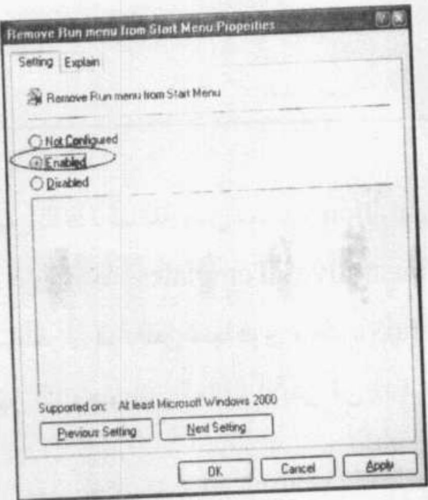
قم بفتح صندوق Run من قائمة start ثم اكتب داخله gpedit.msc ثم انقر OK لتفتح لك نافذة برنامج Group Policy كما بالشكل التالى :



من الجانب الأيسر للنافذة السابقة ومن تحـــت User Configuration قم بالنقر مرتين فوق المجلد Administrative Templates ليتفــرع منه عدة مجلدات أخرى قم بالنقر منها فوق مجلـــد Start Menu and Taskbar ليظهر لك محتوياته بالجانب الأيمن من النافذة كما يلى :

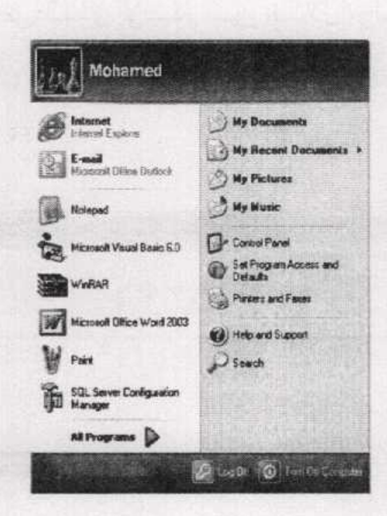


قم بالبحث عـــن البنـــد Remove Run menu from Start Menu الموضح لك بالشكل السابق ثم انقر فوقه مرتين بالماوس لتظهـــر لـــك النافذة التالية :

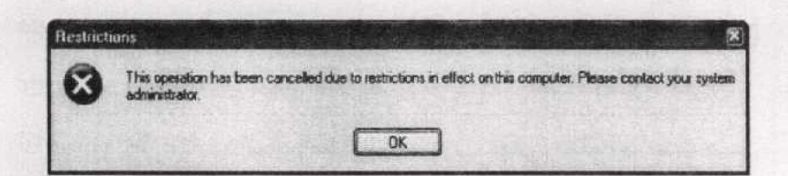


من النافذة السابقة قم بإختيار Enabled ثم نقر Ok .

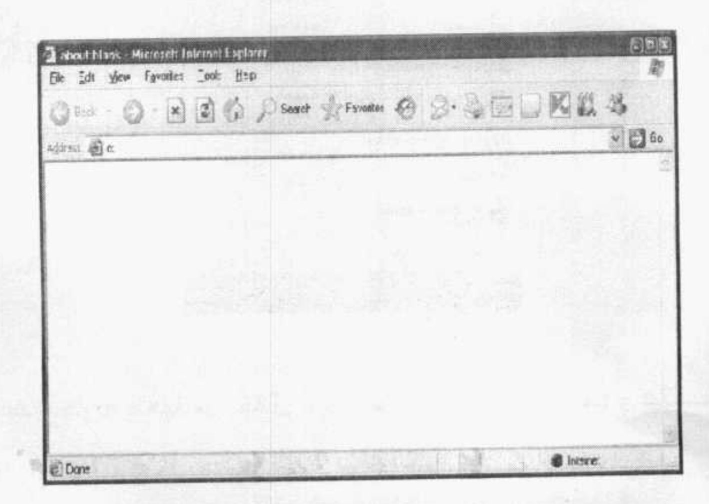
والأن عند ذهابك إلى قائمة start وفتحها لن تجد Run كمـا بالـشكل التالى :



وعند محاولة فتحها من خلال لوحة المفاتيح عن طريق مفتاح علامـة الويندوز ومفتاح R ستظهر لك الرسالة التالية :



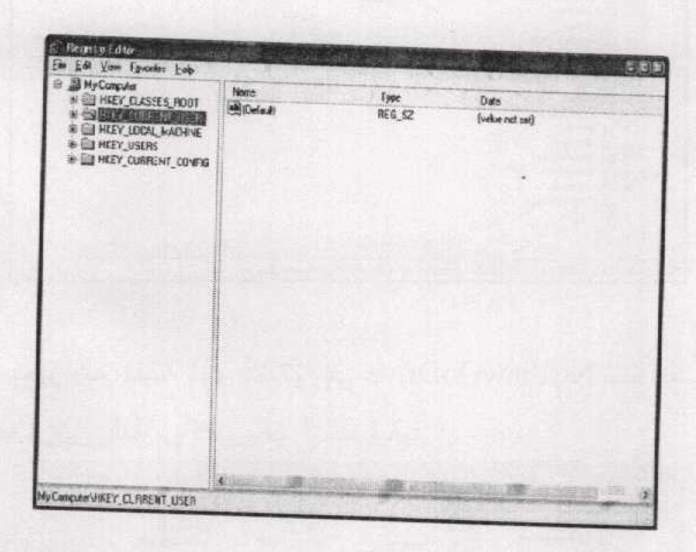
ولكن فى الحقيقة نحن بذلك لم نحل المشكلة بل على العكس أصبح لدينا مشكلة جديدة أخرى وهى أننا نحن أيضاً لن نتمكن من تشغيل صندوق Run هذا بالإضافة أن المشكلة الأولى مازالت قائمة وهى أنه يمكن الوصول إلى القرص الذى أريده من خلال برنامج Internet Explorer مثل أن تكتب فى العنوان رمز القرص ثم اضغط Enter كما بالشكل التالى :



فكر فى حل لهذه المشكلة بشرط أن ألا تقول لى نقوم بإخفاء برنامج Internet Explorer فنحن لا نريد أن نزيد عدد المشاكل مرة أخرى !
إذا لم تجد حل مناسب لهذه المشكلة فأعتقد أن الفكرة التالية ستنقذك من هذا المأزق فتابع معى ...

منع الوصول إلى الأقراص :

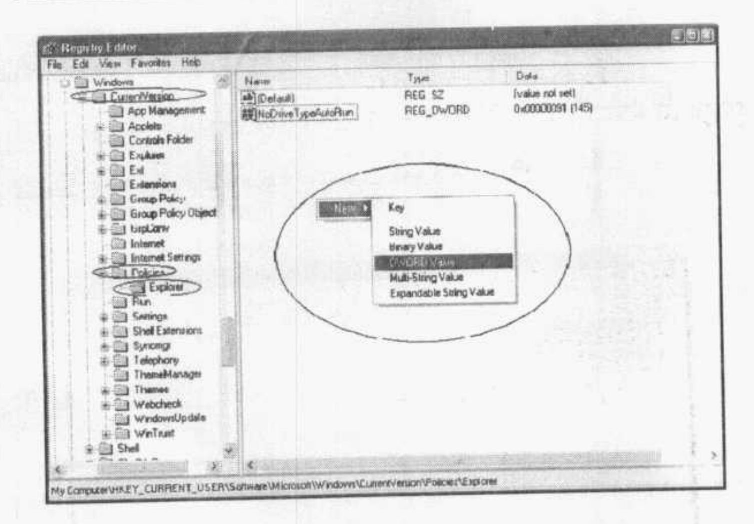
قم بفتح صندوق Run من قائمة Start ثم اكتب regedit واضغط Ok لفتح نافذة محرر السجل كما بالشكل التالى :



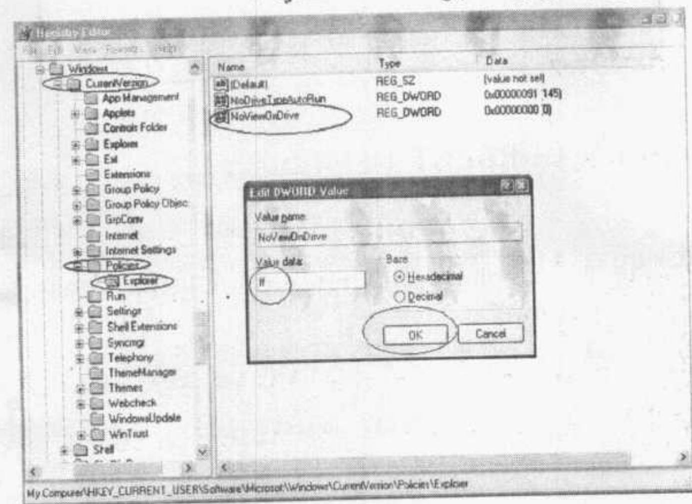
من النافذة السابقة ومن تحت HKEY_CURRENT_USER قم بالذهاب إلى المسار التالى :

Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer

ثم فى الجانب الأيمن من نافذة محرر السجل قم بنقر زر الماوس الأيمن لتظهر لك قائمة من خيار واحد هو New ومنه قم بإختيار DWORD Value كما بالشكل التالى :

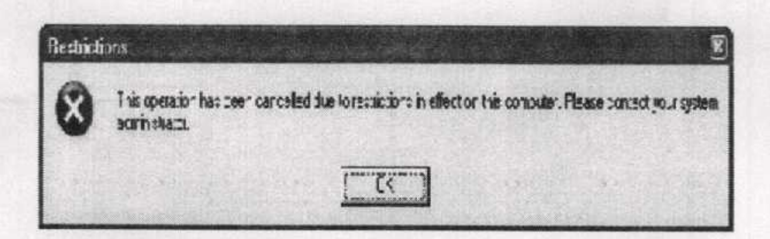


قم بتغيير اسم القيمة الذى أنشأتها إلى NoViewOnDrive ثـم أنقـر فوقه مرتين بالماوس لتظهر لك النافذة التالية :



قم الأن بجعل القيمة تساوى ff كما موضح لك ثم انقر زر Ok ثم أعـــد تشغيل الجهاز .

والأن ليس هناك حاجة لإخفاء الأقراص فقم بإظهارها مرة أخرى وأنت مطمئن لأن أى شخص سيحاول الوصول إليها أوفتحها لن يتمكن مـــن ذلك وستظهر له الرسالة التالية :

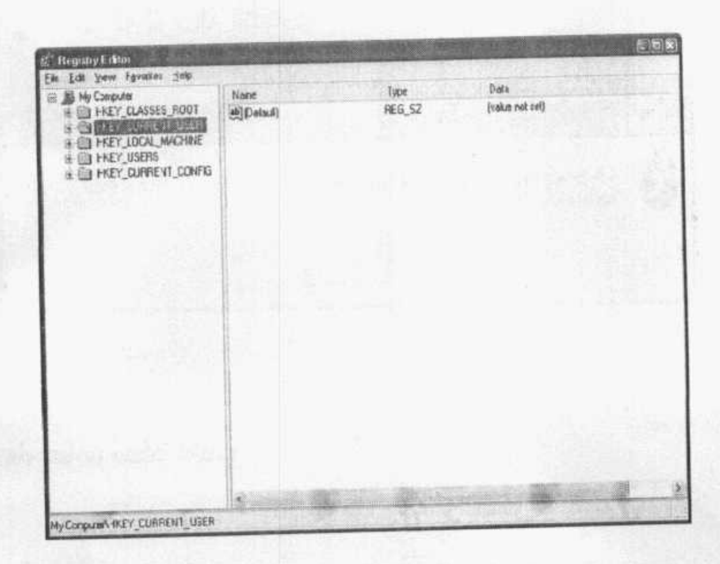


إخفاء عناصر سطح المكتب :

من الأشياء الهامة كذلك إخفاء عناصر سطح المكتب وما يمكن أن يكون فوقه من ملفات هامة وهذه طريقة جيدة تستطيع بها إبعـــاد أى متسلل خطوة أخرى عن هدفه وجعل مهمته أكثر صعوبة ويمكنك ذلـــك بإتباع أى طريقة مما يلى :

الطريقة الأولى :

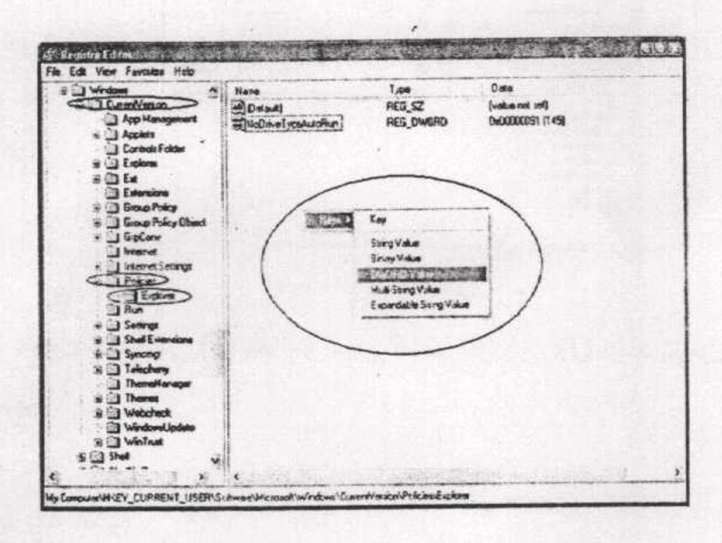
وتتم من خلال محرر السجل فقم بفتحه عن طريق قائمة start واختر منها Run ثم اكتب regedit واضغط Enter أو انقـــر زر Ok لتفتح نافذة محرر السجل كما يلى :



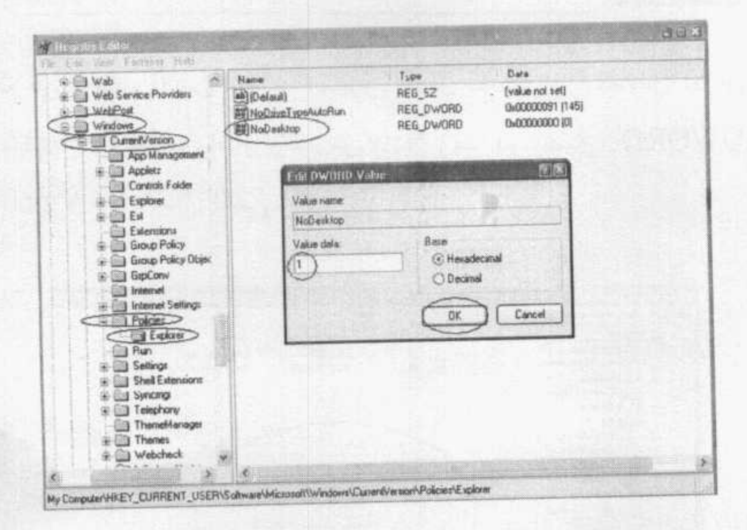
من النافذة السابقة ومن تحــت HKEY_CURRENT_USER قــم بالذهاب إلى المسار التالى :

Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer

ثم فى الجانب الأيمن من نافذة محرر السجل قم بنقر زر الماوس الأيمن لتظهر لك قائمة من خيار واحد هو New ومنه قم بإختيار DWORD Value كما بالشكل التالى :



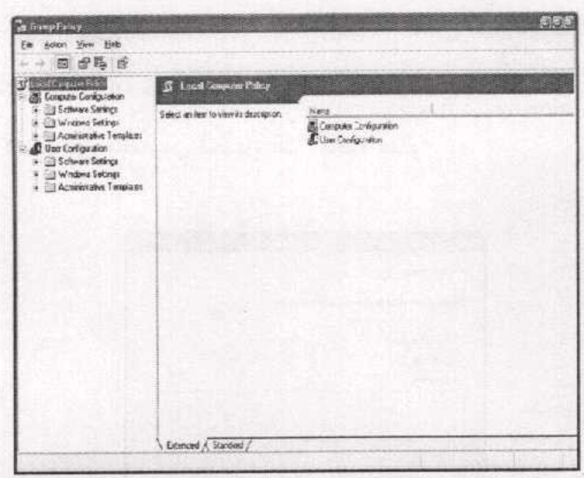
قم بتغيير اسم القيمة الذى أنشأتها إلى NoDesktop ثـم أنقـر فوقـه مرتين بالماوس لتظهر لك النافذة التالية :



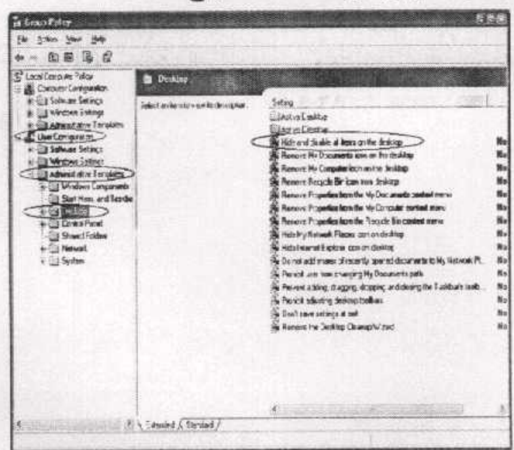
قم بتعديل القيمة إلى (1) كما هو مبين لك ثم انقر زر Ok وأعد تشغيل الجهاز.

الطريقة الثانية :

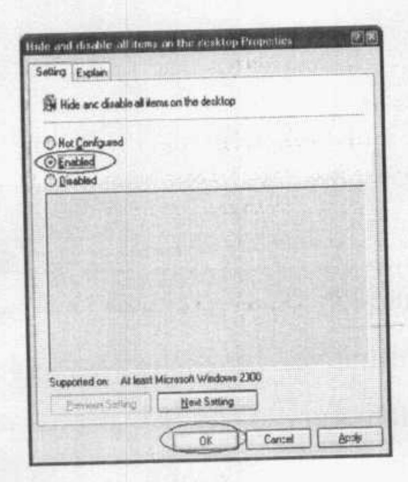
وتتم من خلال Group policy أو سياسة المجموعة فقم بفـــتح صندوق Run من قائمة start واكتب gpedit.msc واضـــغط Enter أو انقر زر Ok لتظهر لك كما يلى :



من الجانب الأيسر للنافذة السابقة ومن تحـــت User Configuration قم بالنقر مرتين فوق المجلد Administrative Templates ليتفـــرع منه عدة مجلدات أخرى قم بالنقر منها فوق مجلد Desktop ليظهر لك محتوياته بالجانب الأيمن من النافذة كما يلى :



من الجانب الأيمن للنافذة السابقة قم بالبحـــث عـــن البنـــد Hide and disable all items on the desktop الموضح لك بالشكل السابق ثم انقر فوقه مرتين بالماوس لتظهر لك النافذة التالية :



كما مبين لك بالشكل السابق قم باختيار Enabled ثم اضغط Ok وأعد تشغيل الجهاز .

الفصل الثامن

حماية الملفات

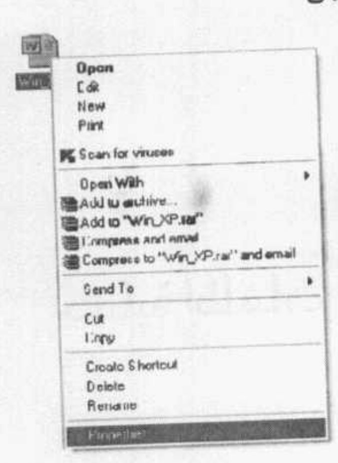
حماية الملفات

بعد أن تعلمت كيف تقوم بحماية الأقراص الصلبة وتأمينها وبأكثر من طريقة قد تجد أنه لاداعى لحماية الملفات نفسها ولكنى سأقوم بما هو واجب على ، ثم عليك أنت أن تقرر ما هو مناسب لك ولكن واجبى أيضاً أن أحذرك مرة أخرى من التراخى وعواقبه ...

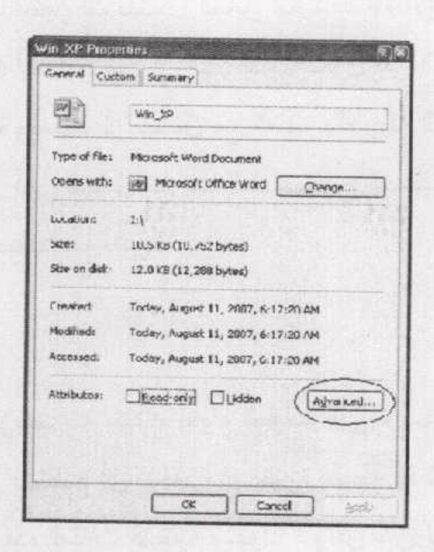
تشفير الملفات :

يتيح لك ويندوز اكس بى ميزة أن تقوم بتشفير أى ملف تريده من خلال الخطوات التالية :

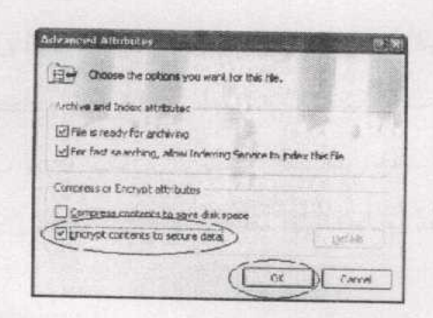
قم بنقر زر الماوس الأيمن فوق الملف الذى تريد تشفيره لتظهر لك قائمة مختصرة كما يلى :



قم باختيار Properties كما موضح لتظهر لك النافذة التالية :



قم بالنقر فوق زر Advanced لتظهر لك نافذة أخرى كما يلى :

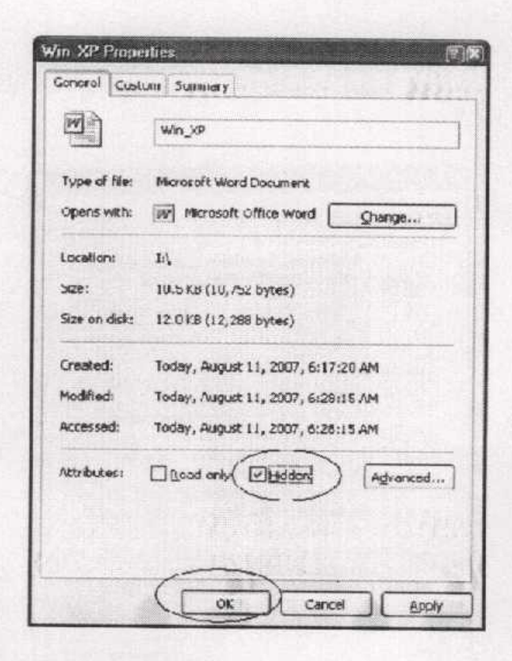


قم بالتأشير فى مربع الخيار Encrypt contents to secure data ثم انقر زر Ok كما يظهر لك بالشكل السابق لتعود للنافذة الأولى لتنقر زر OK الخاص بها أيضاً وستجد أن اسم الملف تحول إلى اللون الأخضر دليل على تشفيره ويمكنك أن تتعامل مع الملف بالطريقة العادية ولكـــن إذا حاول شخص أخر التعامل مع هذا الملف خارج الحساب الخاص بك فلن يستطيع أن يستفيد منه بشىء ...

إخفاء الملفات :

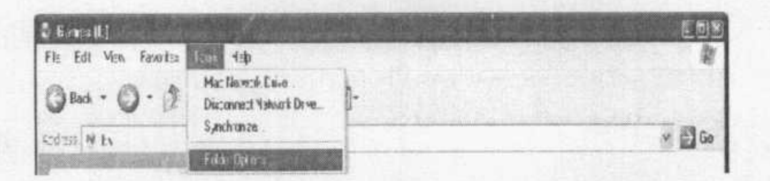
من المعروف أنه يمكنك إخفاء الملفات التى تريدها كنوع مـــن الحماية وإن كان يستطيع أى شخص ذو خبرة بسيطة بإستخدام الحاسب أن يقوم بإظهار هذه الملفات المخفية بسهولة ! ولكن كان لا يمكن لنا أن نغفل مثل هذه النقطة هنا وفى سياق هذا الكتاب الذى نستخدم من خلاله كل ما هو متاح لنا من أدوات حماية وتأمين كما أنه ربما يكون هنـــاك من لايعرف مثل تلك المعلومة ممن يخطون أولى خطواتهم فى إستخدام الحاسب أما أصحاب الخبرة فأقول لهم أنه إذا كنت تبحث عن مـــستوى تأمين جيد فيجب عليك إستخدام كل طرق التـــأمين جنبـــاً إلـــى جنـــب والإستفادة من كل ما هو متاح لك ... أما الأن فهيا بنا لنقوم بإخفاء أحد الملفات .

قم بنقر زر الماوس الأيمن فوق الملف الذى تريد إخفائه لتظهـــر لـــك قائمة مختصرة فقم بإختيار Properties منها كما بينا من قبل لتظهـــر لك هذه النافذة مرة أخرى .

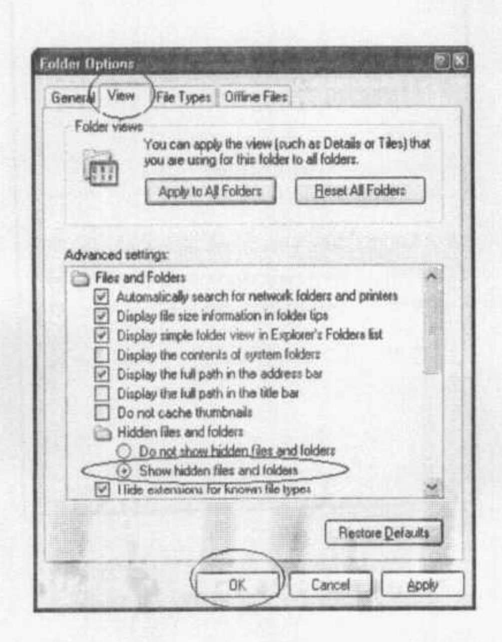


فى هذه المرة من النافذة السابقة سنقوم بالـــتأشير فـــى مربـــع الخيـــار Hidden كما وضح ثم انقر الزر Ok ليتم إختفاء الملف أمـــا إذا أردت إظهاره مرة أخرى فقم بالتوجه لقائمة Tools لأى من نوافذ الوينـــدوز واختر منها Folder Options كما بالشكل التالى :





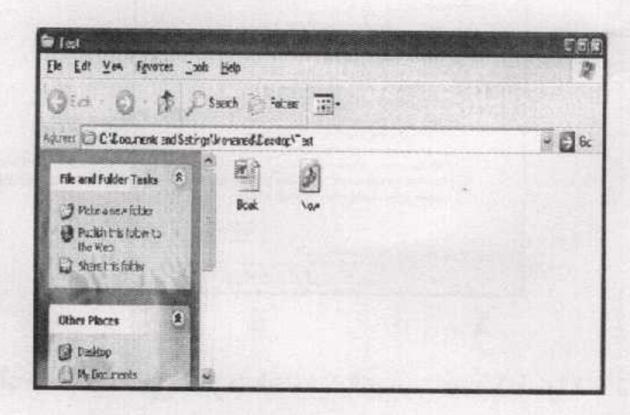
لتظهر لك النافذة التالية :



من النافذة السابقة ومن خلال التبويب View قم بتنشيط الخيار Show hidden files and folders كما موضح لك ثم انقر الزر Ok .

إخفاء إمتداد الملفات :

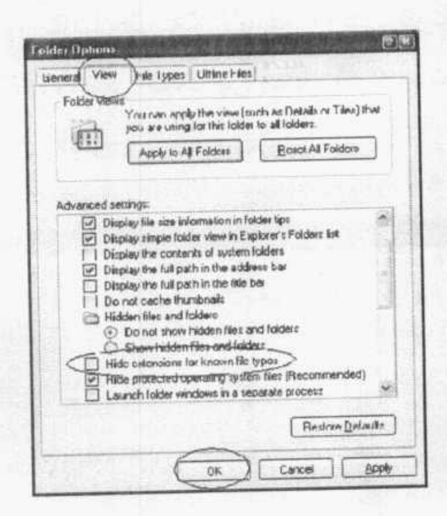
يحتوى كل نوع من أنواع الملفات على إمتداد خاص بـــه هـــذا الإمتداد عبارة عن ثلاثة أحرف ومن خلال هذه الأحرف يتعرف نظـــام التشغيل على نوع هذا الملف وعلى البرنامج المسئول عن تشغيله فمثلا ملفات Word تأخذ الإمتداد (doc) وهكذا لكل ملف الأمتداد الخاص به ويتعرف الويندوز تلقائياً على هذه الإمتدادات وعلى البرنامج المشغل لها ويقوم بتغيير شكل ومظهر الملف إلى مظهر البرنامج المـــسئول عـــن تشغيله كما بالشكل التالى :



كما يتضح لك من الشكل السابق يوجد ملفان يختلف شكل كل منهم عن الأخر ،فأحدهم ملف صوت والأخرمستند وقد قام الويندوز بإعطاء كـــل

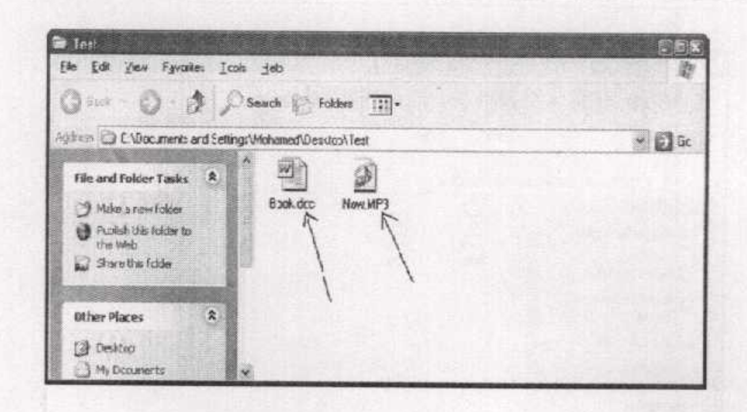
واحد الشكل الذى يتناسب مع نوعه ولكىْ تتمكن من إظهار إمتـــداد أى ملف اتبع الخطوات التالية .

قم بفتح قائمة Tools لأى من نوافذ الويندوز واختـــر منهـــا Folder Options لتظهر لك النافذة التالية والتى تعاملنا معها من قبل .

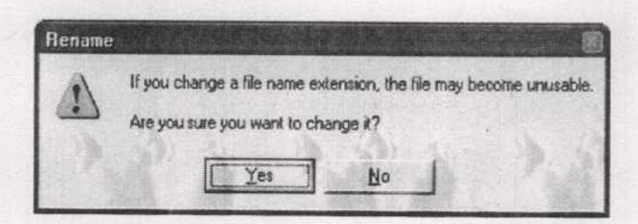


من النافذة السابقة فى الجزء الخاص بالتبويب View قم بإلغاء تنـــشيط المربع الخاص بالخيار Hide extensions for known file types كما موضح ثم انقر الزر Ok .

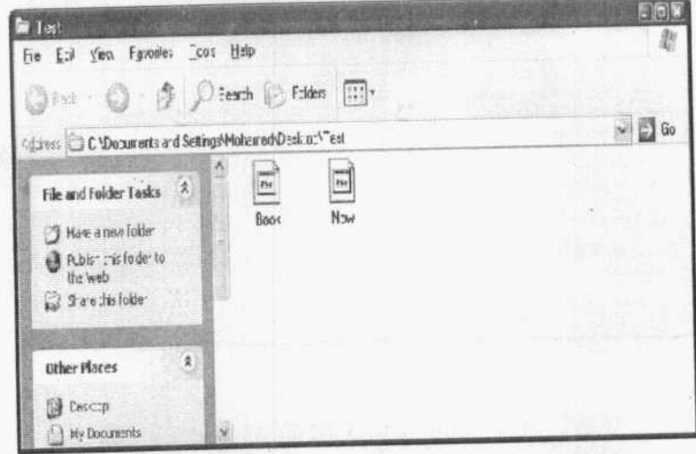
والأن إذا عدت للملفين السابقين ستجد الإمتداد الخاص بكل منهم ظهـــر كما يلى .



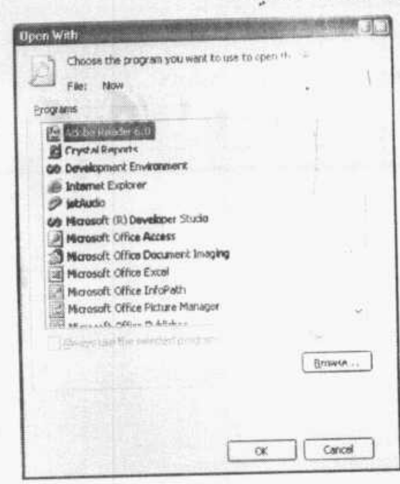
والأن هو الجزء الأهم بالنسبة لنا قم بتحديد أحد الملفين ثم اضـــغط زر F2 من لوحة المفاتيح ثم قم بحذف الإمتداد الخاص بهذا الملف واضغط Enter لتظهر لك الرسالة التالية :



انقر زر yes للرسالة السابقة ثم كرر نفس الخطوات مع الملف الأخـــر ليصبح الشكل كما يلى .



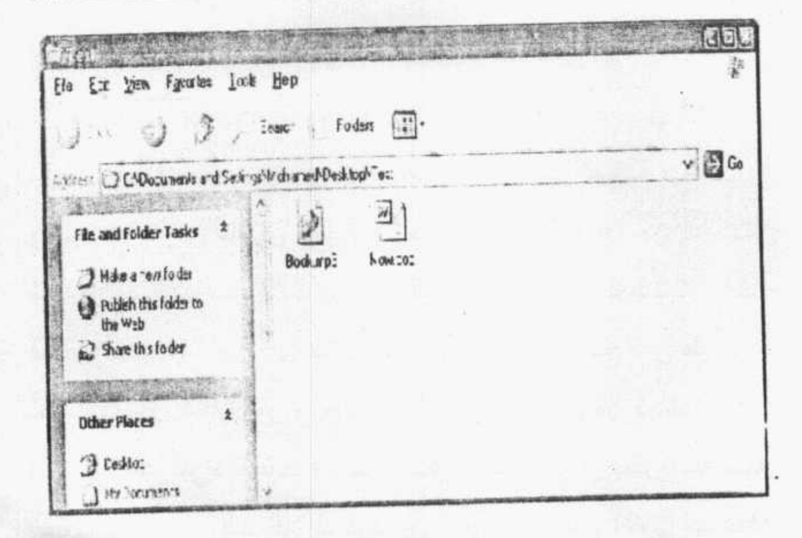
كما ترى فقد تساوى الملفين فى الشكل وهذا الشكل دليل على ان الويندوز لا يستطيع التعرف على نوع تلك الملفات وبالتالى البرنامج المسئول عن تشغيلهم وإذا بالنقر مرتين فوق أى منهم لمحاولة تشغيله أو فتحه ستظهر لك النافذة التالية:



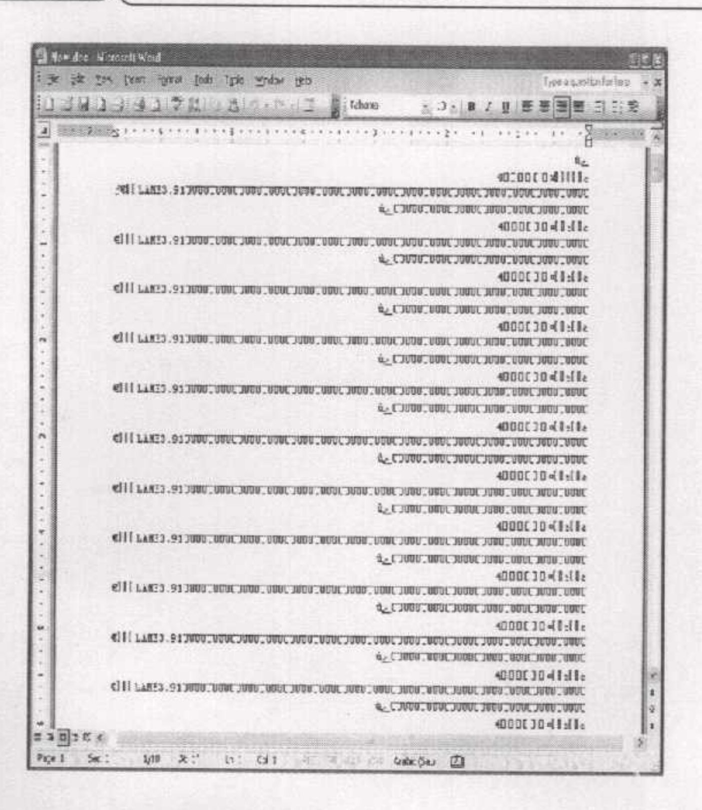
ولاحظ أنك إذا لم تقم بحذف إمتداد الملفات وإنما فقط قمت بتغييره إلـى أى حروف لا تنتمى أو ترمز إلى أى نوعية من البرامج مثل ttt أو أى شىء من هذا القبيل ستحصل أيضاً على نفس النتيجة السابقة .

وهذه الطريقة من الطرق الجيدة جداً فى التأمين والخداع ولكن إذا كـان أحد هؤلاء الأشخاص يشك فى هذا الملف وأن بـه معلومـات هامـه فسيقوم بتجربة تشغيل هذا الملف عن طريق أحد البرامج التى ظهـرت أمامك بالشكل السابق وربما ظل يحاول إلى أن يتمكن من تـشغيله قـد تعتقد أن ذلك شىء مستبعد ولكنك لا تعرف ما يمكن أن يفكر بـه مـن يحاول التلصص عليك فلا بد دائماً أن تفترض الأسوء لتكون مـستعداً ... ولذلك ما رأيك أن نقوم بحيلة أخرى تطمن لنا مزيد مـن التمويـه والحصول على نتيجة أفضل .. فتابع معى ...

سنقوم فى هذه الفكرة بإرجاع الإمتداد مرة أخرى ولكـن مـع إبـدال الملفات بمعنى أن نقوم بوضع إمتـداد (mp3) إلـى ملـف ال Word وإمتداد (doc) إلى ملف الصوت ليصبح الشكل كما يلى :



لاحظ تحول شكل كل ملف إلى نوع الإمتـداد الـذى يحملـه واصـبح المظهر طبيعى ولا يثير فضول أو يلفت إنتباه أحد ولكن عنـد تـشغيل ملف الصوت Now بعد أن أصبح يحمل إمتداد الملفات النصية كانـت هذه هى النتيجة .



وكذلك عند تشغيل الملف Book بعد أن أصبح يحمل إمتداد الملفات الصوتية لم يحدث شيء ولكن أى شخص أخر لا يعرف ما قمت به وعند حدوث ذلك معه سيظن أن هذه ملفات تالفة وسيتركها ليبحث عن غيرها .

ولكن لا تنسى بعد أن تنتهى من عملك أن تقوم بإخفاء إمتداد الملفات مرة أخرى...



الفصل التاسع

منع التحكم بنظام التشغيل

منع التحكم بنظام التشغيل

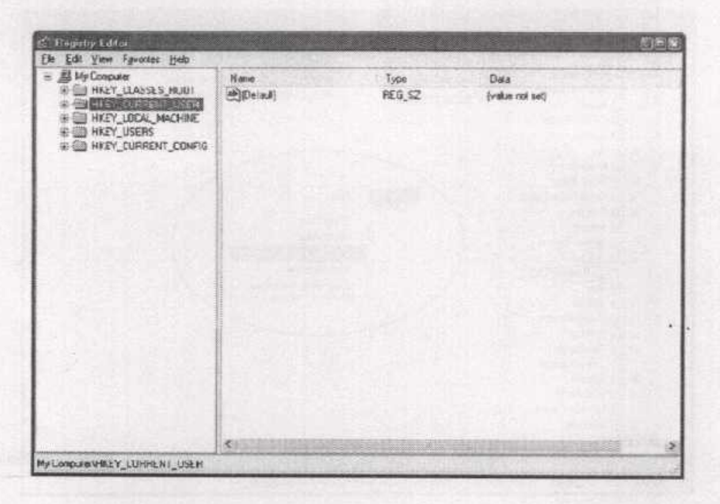
فى هذا الفصل سنتناول موضوع هام جداً يتعلق بنظام التشغيل وما يحويه من برامج فيمكنك أن تقوم بإخفاء قائمة البرامج All Programs من قائمة start أيضاً يمكنك أن تمنع الوصول إلى لوحة التحكم Control panel وقد يكون من المفيد جداً أن تقوم بإستخدام هذه الميزة لتمنع وصول أى شخص إلى لوحة التحكم لأسباب عديدة بغض النظر عن السبب الأمنى فقد تسمح لشخص ما بإستعمال جهازك وتخشى أن يقوم بتغيير أى من الإعدادات أو البرامج أو أى شيء من هذا القبيل دون قصد .. أما إذا عدت إلى السبب الأمنى فستجد أنه شيء ضرورى جداً أن تقوم بحرمان أى مخترق من الوصول لهذه التحكمات لأنه عندما يفشل فى هدفه قد يفكر فى الإنتقام منك بأى طريقة !

منع الوصول إلى لوحة التحكم Control panel :

ويمكن القيام بذلك بتنفيذ أى طريقة مما يلى :

الطريقة الأولى :

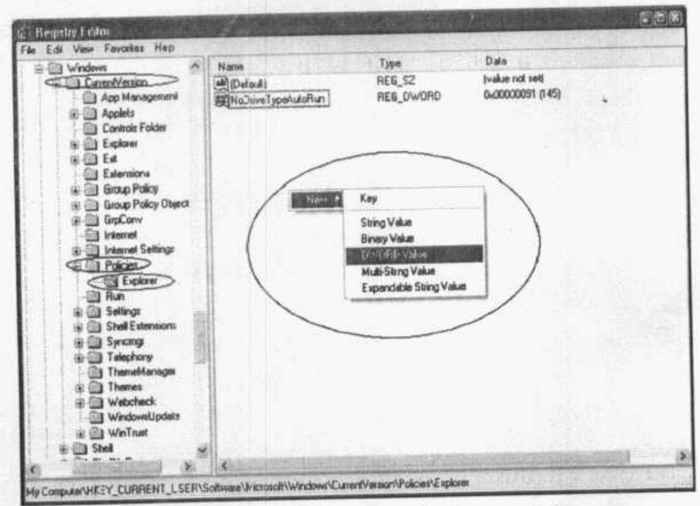
وتتم من خلال محرر السجل فقم بفتحه عن طريقة قائمة start واختر منها Run ثم اكتب regedit واضغط Enter أو انقر زر Ok لتفتح نافذة محرر السجل كما يلى :



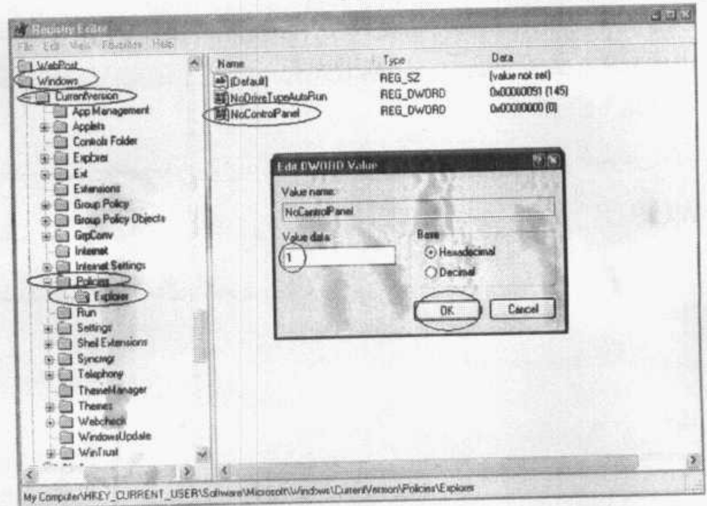
من النافذة السابقة ومن تحـت HKEY_CURRENT_USER قـم بالذهاب إلى المسار التالى :

Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer

ثم فى الجانب الأيمن من نافذة محرر السجل قم بنقر زر الماوس الأيمن لتظهر لك قائمة من خيار واحد هو New ومنه قم بإختيار DWORD Value كما بالشكل التالى :



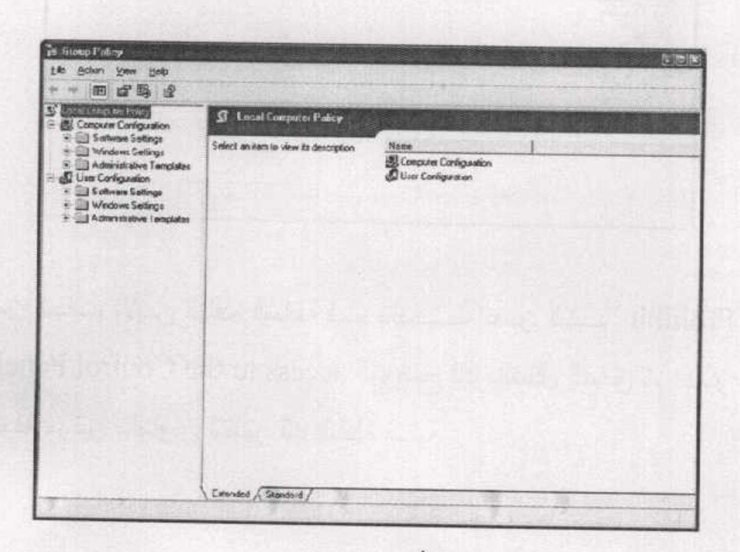
قم بتغيير اسم القيمة الذى أنشأتها إلى NoControlPanel ثم أنقر فوقه مرتين بالماوس لتظهر لك النافذة التالية :



قم بتعديل القيمة إلى (1) كما هو مبين لك ثم انقر زر Ok وأعد تشغيل الجهاز.

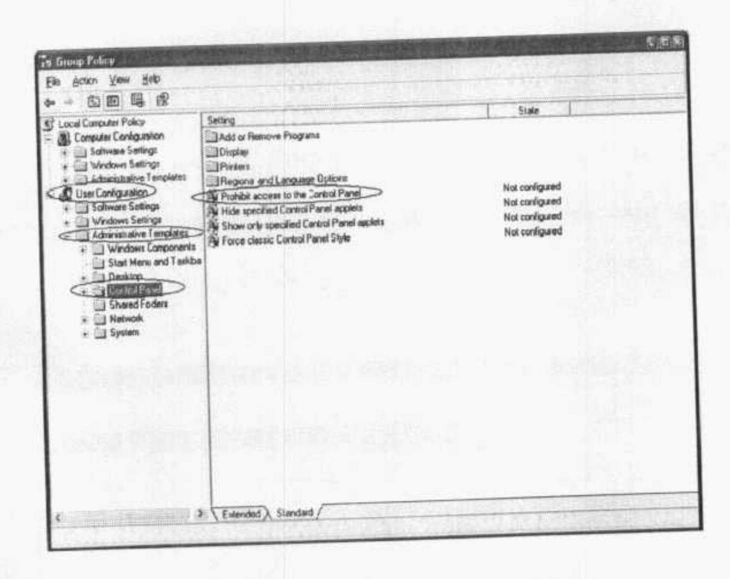
الطريقة الثانية :

وتتم من خلال Group policy أو سياسة المجموعة فقم بفتح صندوق Run من قائمة start واكتب gpedit.msc واضغط Enter أو انقر زر Ok لتظهر لك كما يلي :



من الجانب الأيسر للنافذة السابقة ومن تحت User Configuration قم بالنقر مرتين فوق المجلد Administrative Templates ليتفرع

منه عدة مجلدات أخرى قم بالنقر منها فـــوق مجلـــد Control panel ليظهر لك محتوياته بالجانب الأيمن من النافذة كما يلى :

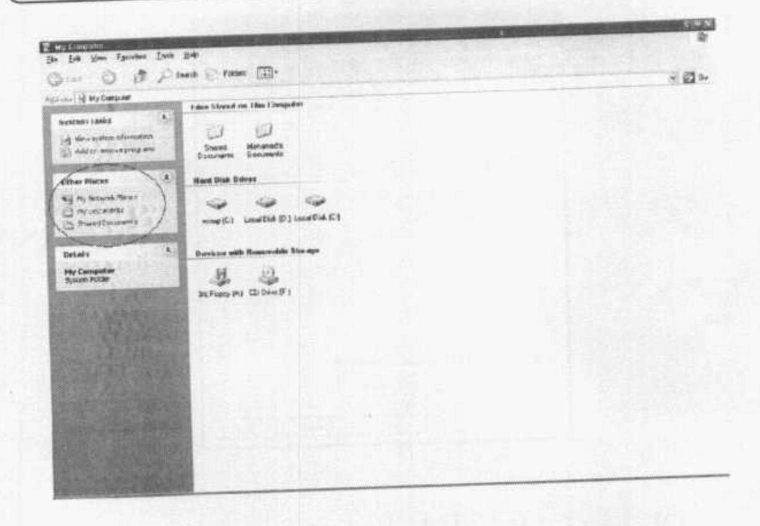


من الجانب الأيمن للنافذة السابقة قـــم بالبحـــث عـــن البنـــد Prohibit access to the Control Panel الموضح لك بالشكل السابق ثم انقـــر فوقه مرتين بالماوس لتظهر لك النافذة التالية :

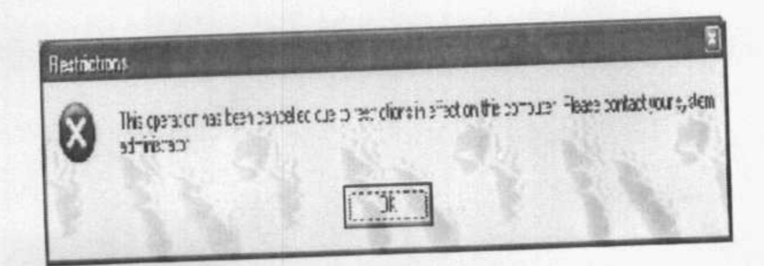


كما مبين لك بالشكل السابق قم باختيار Enabled ثم اضغط Ok .

لاحظ بعد إستخدامك لأى من الطريقتين سيتم إختفــاء Control Panel من قائمة start ومن نافذة My computer كما بالشكل التالى :



وعند محاولة الوصول إلى Control Panel بأى طريقة أخرى ستظهر رسالة الإعتراض التالية

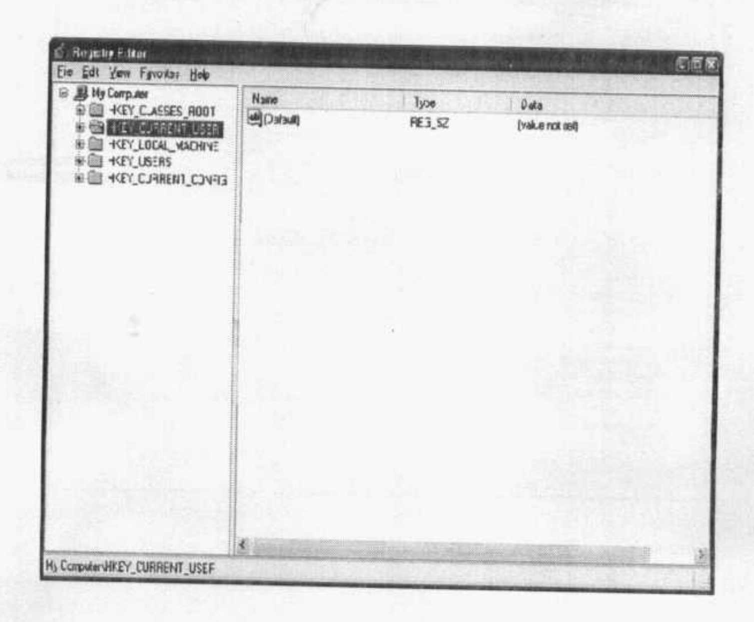


إزالة البرامج من قائمة start :

من الأشياء الهامة أن تقوم بإخفاء قائمة برامجك من قائمة بـــدء التشغيل لتمنع بذلك الوصول إلى تلك البرامج أو العبث بهـــا وكالعـــادة سنتناول أكثر من طريقة لعمل ذلك كما يلى :

الطريقة الأولى :

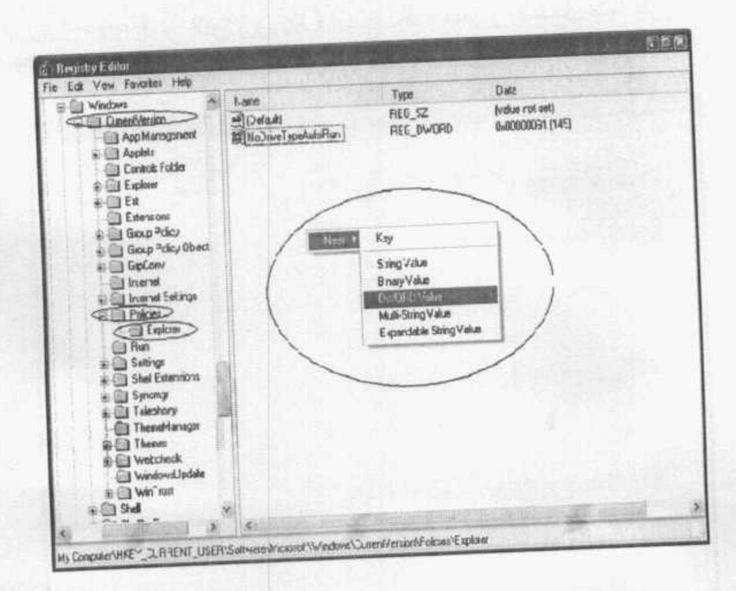
قم بفتح صندوق Run من قائمة start ثم أكتب الأمر regedit واضغط Enter أو انقر زر Ok لتفتح نافذة محرر السجل كما يلى :



من النافذة السابقة ومن تحـــت HKEY_CURRENT_USER قــم بالذهاب إلى المسار التالى :

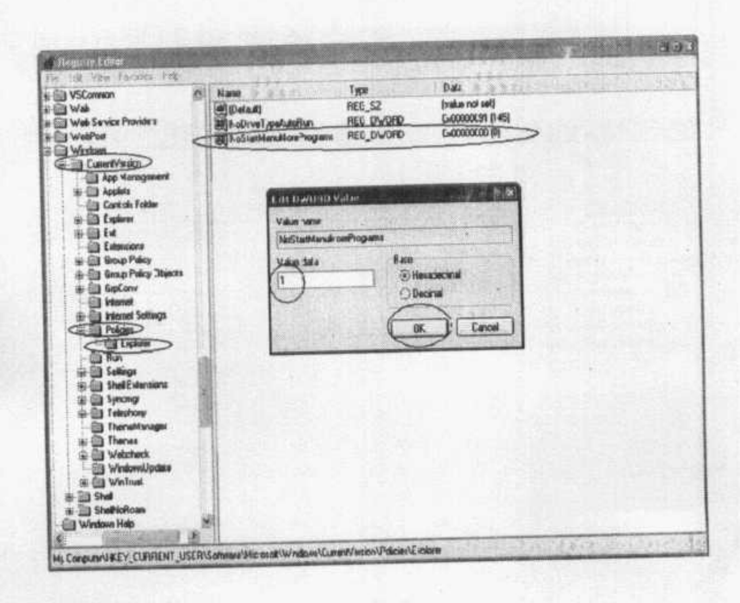
Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer

ثم فى الجانب الأيمن من نافذة محرر السجل قم بنقر زر الماوس الأيمن لتظهر لك قائمة من خيار واحد هو New ومنه قم بإختيار DWORD Value كما بالشكل التالى :



قم بتغيير اسم القيمة الذى أنشأتها إلى:

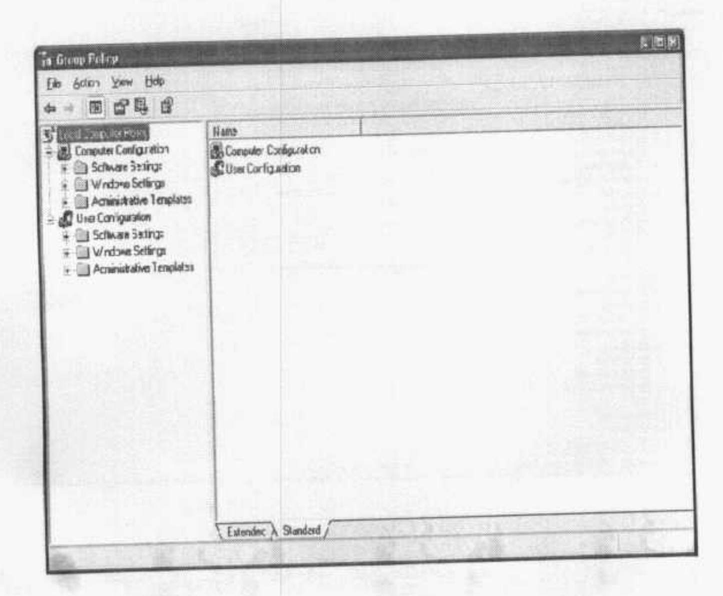
NoStartMenuMorePrograms ثم أنقر فوقه مـــرتين بالمـــاوس لتظهر لك النافذة التالية :



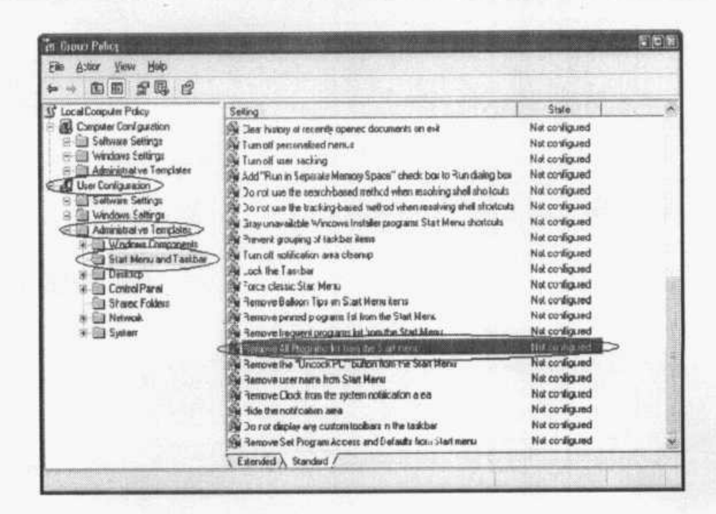
قم بتعديل القيمة إلى (1) كما هو مبين لك ثم انقـــر زر Ok ثـــم أعـــد تشغيل الجهاز .

الطريقة الثانية :

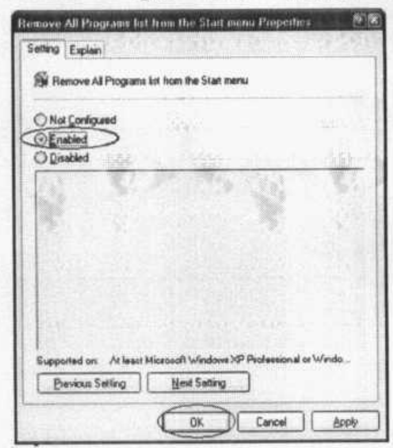
وتتم من خلال Group policy أو سياسة المجموعة فقم بفـــتح صندوق Run من قائمة start واكتب gpedit.msc واضـــغط Enter أو انقر زر Ok لتظهر لك كما يلى :



من الجانب الأيسر للنافذة السابقة ومن تحـــت User Configuration قم بالنقر مرتين فوق المجلد Administrative Templates ليتفـــرع منه عدة مجلدات أخرى قم بالنقر منها فوق مجلـــد Start Menu and Taskbar ليظهر لك محتوياته بالجانب الأيمن من النافذة كما يلى :



قم بالبحث فى الجانب الأيمن من النافذة السابقة عـن البنـد Remove All Programs list from the Start menu الموضح لك بالـشكل السابق ثم انقر فوقه مرتين بالماوس لتظهر لك النافذة التالية :



قم بتنشيط الخيار Enabled من النافذة السابقة كما موضح ثم أنقــر زر Ok و أعد تشغيل الجهاز.

وبعد تنفيذك أى طريقة مما سبق قم بفتح قائمة start لتجد إختفاء قائمــة All programs .



الفصل العاشر

ويندوز اكس بى يطرد الغرباء !

ويندوز اكس بى يطرد الغرباء !

سنقوم فى هذا الفصل بتطبيق فكرة رائعة تغنيك عن القيام بتأجير حارس خاص يظل بجوار الحاسب لحمايته من محاولة دخول أى من الغرباء .. فمن خلال هذه الفكرة سنجعل الويندوز هو الحارس على نفسه ! وسنحدد له رد الفعل الذى يقوم به عند دخول أحد الأشخاص إليه مثل أن يقوم بإغلاق الجهاز أو عمل إعادة تشغيله له أو غير ذلك ولكن المشكلة التى ستواجهنا فى ذلك هى أن الويندوز لن يميز فى ذلك بين مستخدم وأخر أى أنه بمجرد دخول أى شخص إلى الجهاز سيقوم برد الفعل هذا حتى وإن كان هذا الشخص هو أنت !! ولذلك سيتعين علينا عند دخولنا إلى الجهاز أن نوقف هذا الإجراء لكى نتمكن من التعامل مع الجهاز أما إذا قام أحد الغرباء بإقتحام الويندوز فسيتم تطبيق هذا الإجراء ويطرد خارج الويندوز والخطوات التالية توضح لنا ما علينا القيام به من أجل تنفيذ ذلك كله .

1- عمل برنامج دفعى يقوم بإغلاق الويندوز .

2- جعل هذا البرنامج يعمل مع بداية تشغيل الويندوز .

3- إبطال عمل هذا البرنامج بمجرد دخولنا إلى الويندوز لنتمكن من التعامل معه .

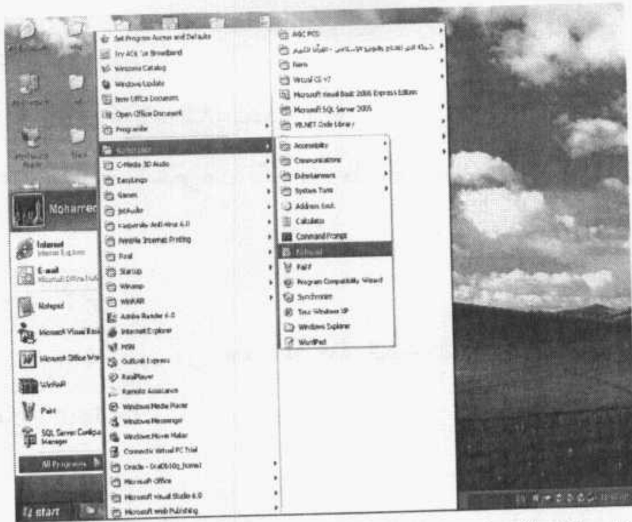
إنشاء الملف الدفعى :

سنقوم أولا بإنشاء الملف الدفعى الذى يحتوى على الأوامر التى نريدها وكالعادة سنستعرض أكثر من طريقة لإنشاء هذا الملف كما يلى:

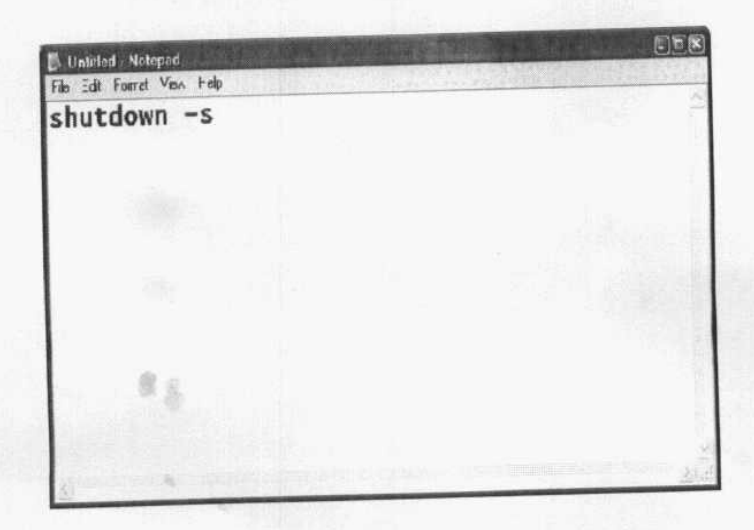
الطريقة الأولى :

سنستعرض فى هذه الطريقة إنشاء الملف الدفعى من خلال برنامج Notepat .

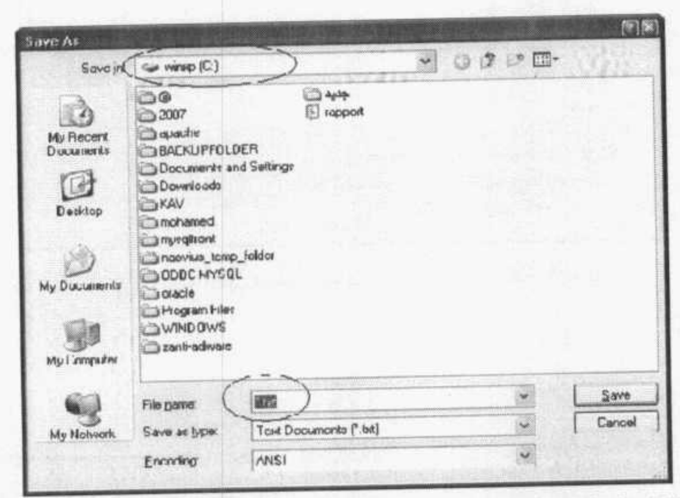
قم بالذهاب إلى قائمة start ثم All Programs ومنها إلى Accessories ثم Notepat كما بالشكل التالى :



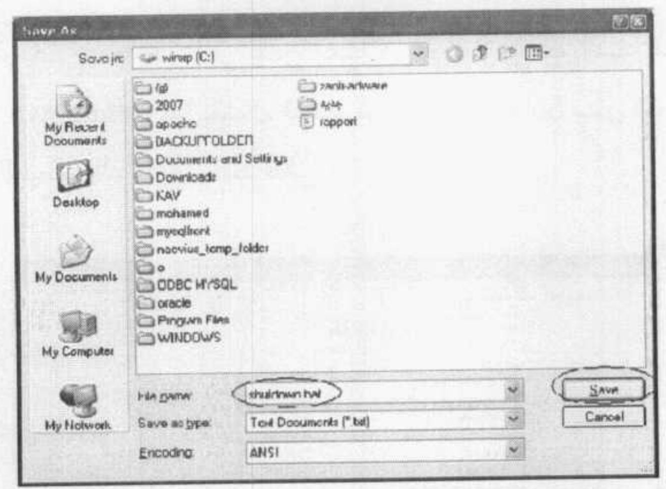
لتظهر لك نافذة البرنامج كما يلى :



ثم قم بكتابة الأمر المسئول عـن إغـلاق الجهـاز وهـو كمـا يلـى shutdown –s وكما بالشكل السابق ثم قم بإختيار Save مـن قائمـة File ليظهر لك مربع الحفظ التالى :



من القائمة المنسدلة بجوار Save in قم بتحديد مكان حفظ الملف ثم من القائمة المنسدلة بجوار File name قم بكتابة أى اسم للملف بـشرط أن يكون الإمتداد هو Bat كما بالشكل التالى :



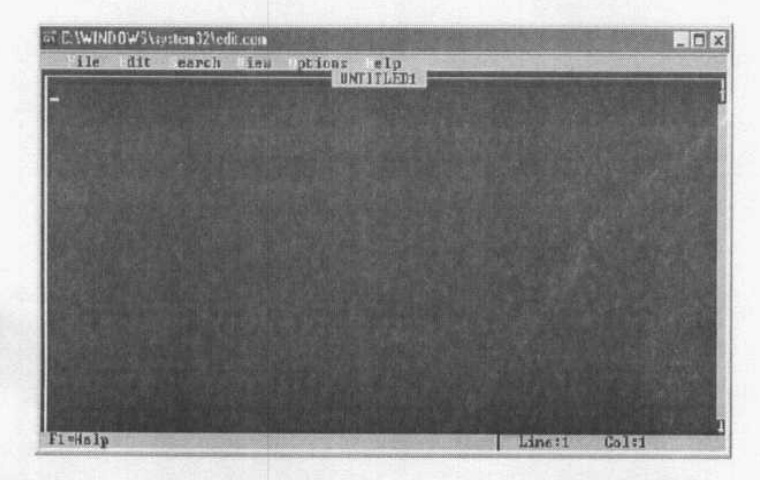
ثم بعد ذلك انقر زر Save لحفظ الملف وسيصبح شكله كما يلى :



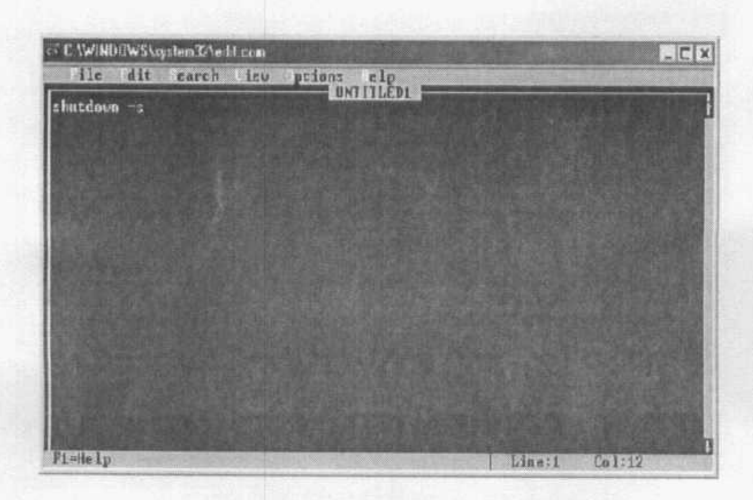
الطريقة الثانية :

سنقوم من خلال هذه الطريقة بإنشاء الملف عن طرق الـــدوس Dos .

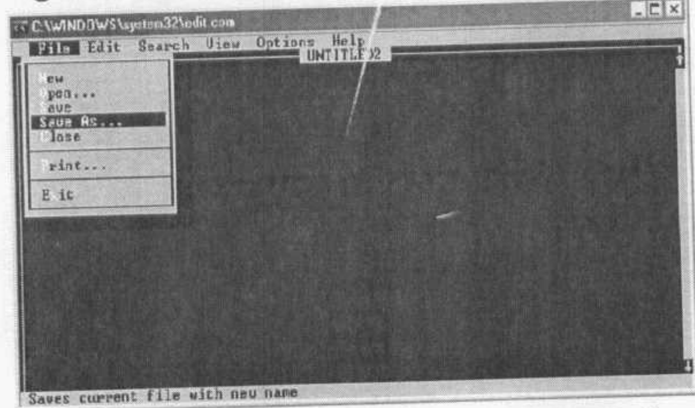
قم بفتح صندوق Run من قائمة start ثم اكتب الأمر edit لتفتح لـــك نافذة محرر نصوص الدوس كما بالشكل التالى :



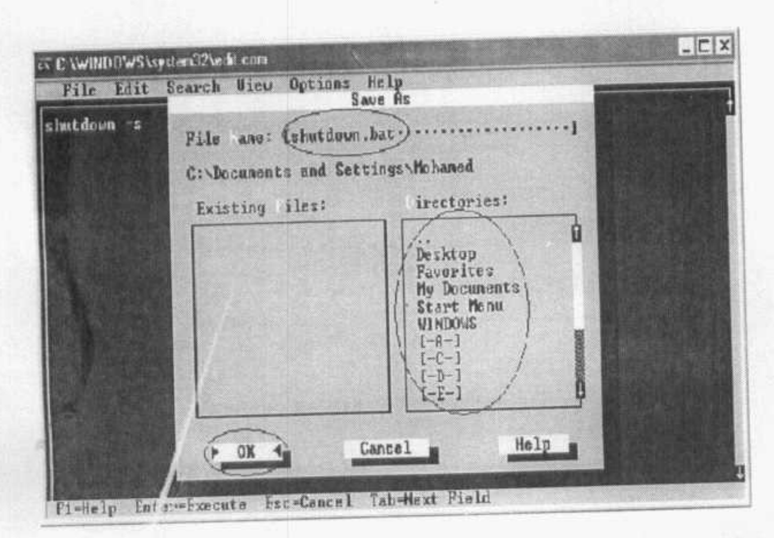
قم الأن بكتابة أمر إغلاق الجهاز shutdown –s لتصبح نافذة البرنامج كما يلى:



ثم قم بالذهاب لقائمة File واختر منها Save as كما بالشكل التالى :



لتظهر لك النافذة التالية :



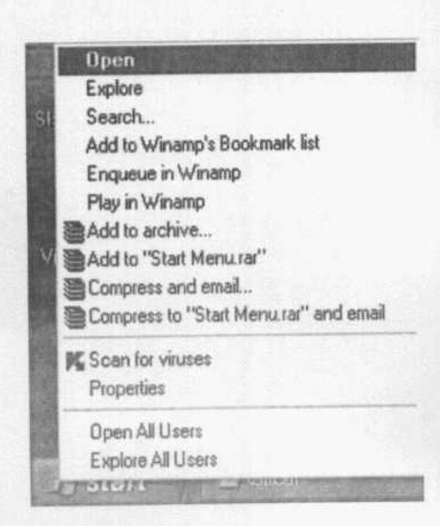
قم بكتابة اسم للملف فى الجزء بجوار File Name وبنفس الشرط السابق أن يكون بإمتداد Bat ومن أسفل الجزء Directories حدد مكان حفظ الملف ثم انقر زر Ok كما يتضح لك من الشكل السابق لنكون بذلك إنتهينا من هذا الجزء.

الملف يعمل مع بداية تشغيل الويندوز :

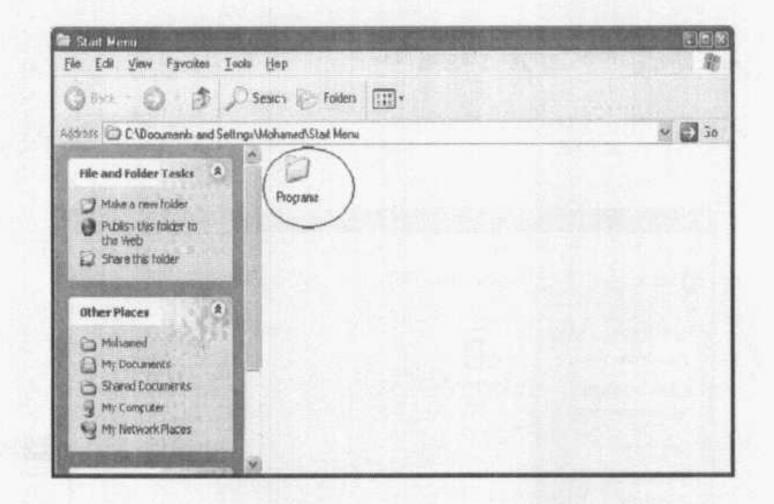
علينا الأن أن نجعل هذا الملف يعمل مع بداية عمل الويندوز ويتم ذلــك بإتباع أى طريقة مما يلى .

الطريقة الأولى :

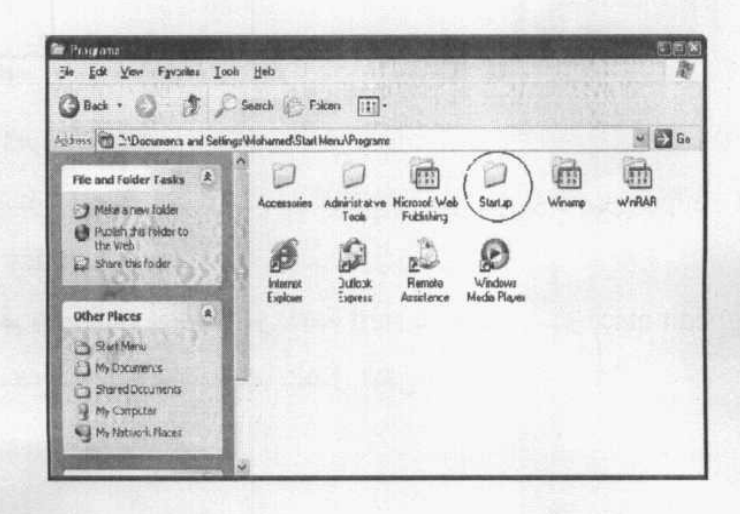
قم بنقر زر الماوس الأيمن فوق قائمة start لتظهر قائمة مختصرة كما يلى :



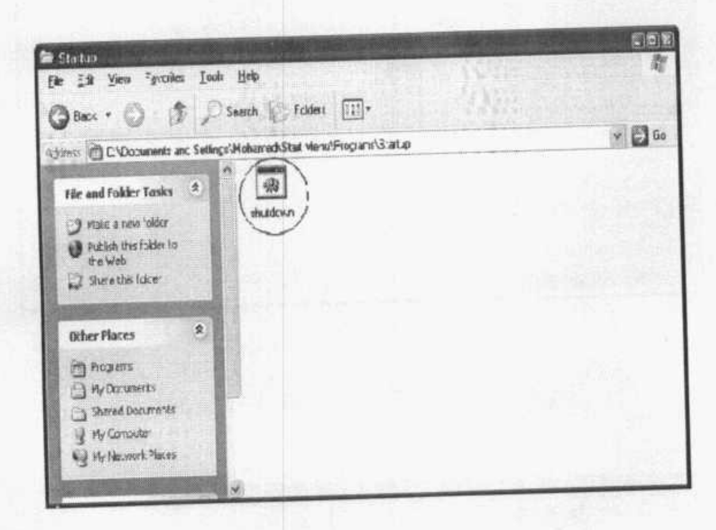
من القائمة السابقة قم بالنقر فوق Open لتفتح لك النافذة التالية :



قم بالنقر مرتين فوق المجلد Programs لفتحه كما يلى :



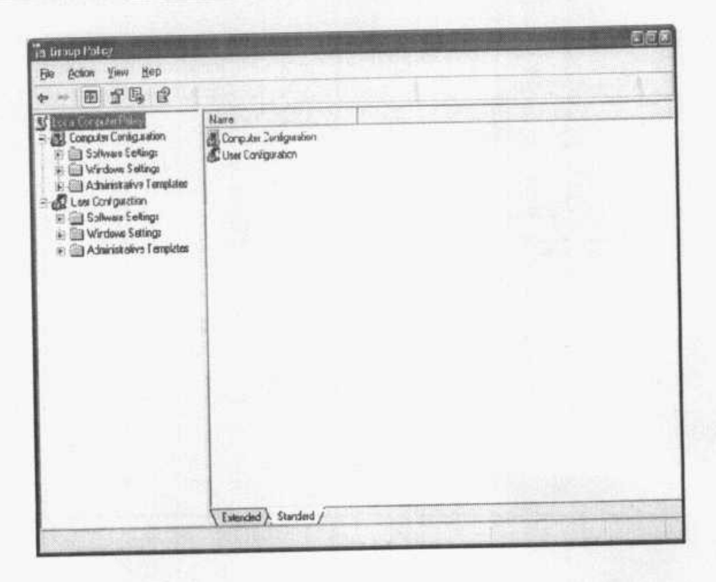
قم بالنقر مرتين فوق المجلد Startup لفتحه ثم قم بنسخ الملف الـــدفعى إلى داخله كما يلى :



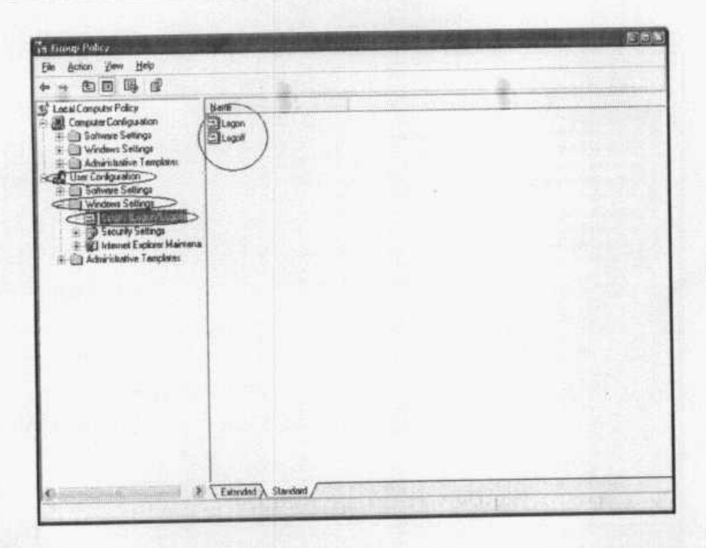
الطريقة الثانية :

سنقوم فى هذه الطريقة بتشغيل الملف عن طريـــق برنـــامج Group Policy فتابع معى ...

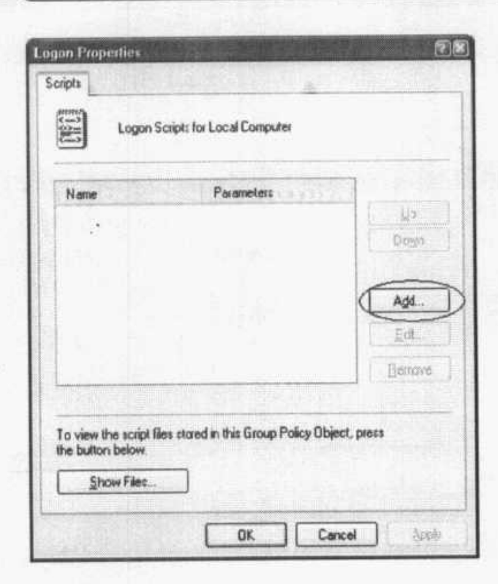
قم بفتح صندوق Run من قائمة start ثم اكتب الأمــــر gpedit.msc لتفتح لك نافذة البرنامج كما بالشكل التالى :



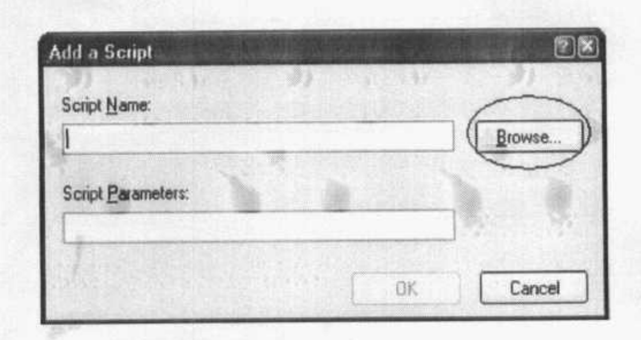
من الجانب الأيسر للنافذة السابقة ومن تحـــت User Configuration قم بالنقر مرتين فوق المجلد Windows Settings ليتفرع منـــه عـــدة تفريعات أخرى قم بالنقر منها فوق[Logon/Logoff] Scripts ليظهر لك محتوياته بالجانب الأيمن من النافذة كما يلى :



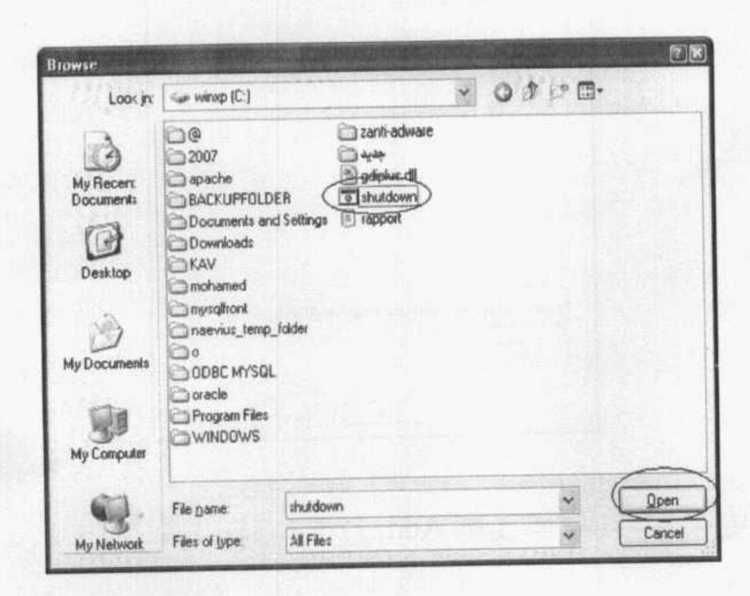
يظهر لك فى الجانب الأيمن للنافذة السابقة بندان أحدهما خاص بالبرامج التى نريدها أن تعمل مع بداية تشغيل الويندوز ودخول المستخدم والأخر خاص بالبرامج التى نريدها أن تعمل عند خروج المستخدم وبالطبع ما يعنينا هنا هو البند الأول والذى بالإسم Logon فقم بالنقر فوقه مرتين بالماوس لتظهر لك النافذة التالية :



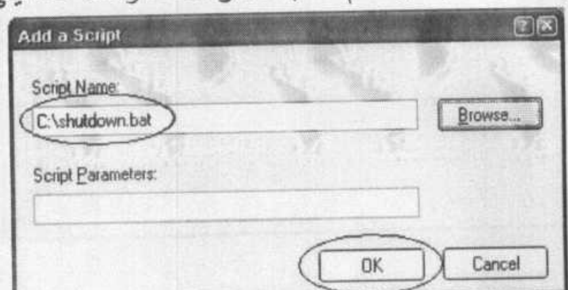
من النافذة السابقة قم بالنقر فوق زر Add لتظهر لك نافذة أخـــر كمـــا يلي:



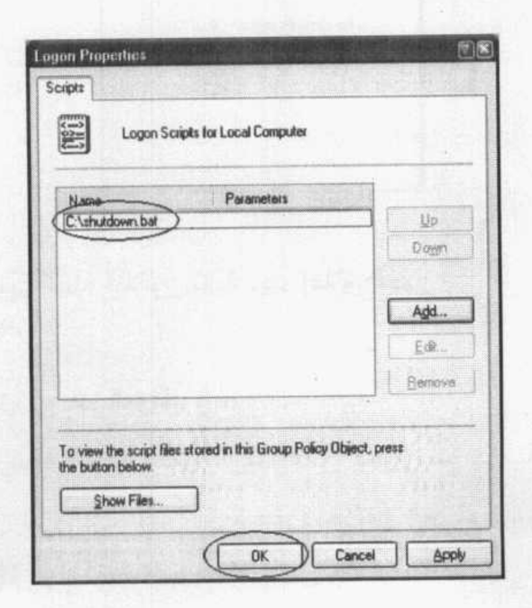
قم بالنقر فوق زر Browse ليفتح لك المربع التالى :



من النافذة السابقة قم بتحديد الملف الذى قمنا بإنشائه ثم انقر زر Open لتعود إلى النافذة السابقة وقد تم تحديد مسار الملف واسمه كما يلى :



قم بنقر زر Ok لتعود للنافذة الأولى وقد أضيف اسم الملف إليها كما يلى :



قم بنقر زر Ok للنافذة السابقة ثم أغلق برنامج Group Policy .
وبمجرد تشغيل الجهاز فى المرة القادمة ستظهر لك الرسالة التالية تخبرك بأن الجهاز سوف يغلق بعد 30 ثانية وتبدأ فى العد التنازلى .



وبعد أن تنتهى مهلة الثلاثون ثانية سيتم إغلاق الجهاز .

كيف نتعامل مع هذا الموقف ؟ :

الرسالة السابقة ستظهر ويتم إغلاق الجهاز مع بداية تشغيل الجهاز ولن تفرق بينك وبين أى شخص أخر من الغرباء لذلك علينا إيجاد طريقة نقوم من خلالها بإبطال عمل هذا الملف الدفعى وبالتالى إختفاء هذه الرسالة لنتمكن نحن من التعامل مع الجهاز ويمكننا القيام بذلك بأكثر من طريقة ولكن الأهم هو أن تفعل ذلك قبل أن تنتهى فترة الثلاثون ثانية ولكن أطمئنك بأنها خطوات بسيطة يمكن تنفيذها فى مدة أقل من ذلك بكثير فتابع معى ...

الطريقة الأولى :

عن طريق صندوق Run نكتب الأمـــر shutdown –a ثـــم نضغط Enter .

الطريقة الثانية :

أن نقوم بإنشاء ملف دفعى أخر كما تعلمنا من قبل ولكن تكـــون القيمة داخله shutdown –a وليس shutdown –s وتـــضعه فـــى أى مكان وعند تشغيل الجهاز تقوم بالذهاب إلى هذا الملـــف وتنقـــر عليـــه مرتين بالماوس .

وعند تنفيذك لأى طريقة مما سبق سيتم إختفاء الرسالة دليل على إبطال مفعول الملف الدفعى الخاص بإغلاق الجهاز .

سؤال هام ؟

قد تقول أن أى شخص أخر إذا تمكن من الدخول للجهاز ووجد هـــذه الرسالة يمكنه أن يفعل نفس الخطوات السابقة وهو بـــذلك يتـــساوى معنا !!!

الجواب العادى :

يمكنك أن تستعمل الطريقة الثانية الخاصة بإنشاء ملـــف دفعـــى لإبطال مفعول الملف الدفعى الخاص بإغلاق الجهاز وحفظه فى مكـــان

بعيد عن متناول أى شخص ثم تقوم بإبطال وإخفاء صندوق Run كما تعلمنا فى جزء سابق من الكتاب وبالتالى عند ظهور تلك الرسالة وحاول أحد الأشخاص إستخدام صندوق Run فلن يتمكن من ذلك وبالطبع لن يتمكن من إنشاء ملف دفعى وحفظه وتشغيله هذا فضلاً عن الوقت الذى ستستغرقه مفاجأة ظهور هذه الرسالة .

الجواب الإحترافى والعملى :

يمكنا أن نقوم بإنشاء ملف دفعى أخر لايقوم بإظهار مثل هذه الرسالة وبالتالى لن يعرف أحد غيرك أن الجهاز سيغلق وعند تشغيلك أنت للجهاز تقوم بإبطال ذلك كما تعلمت من قبل أما إذا كان أحد الغرباء هو الذى تسلل إلى الجهاز فسيجد نفسه مطروداً من قبل الويندوز ودون أن يشعر بما يحدث بل يوجد ما هو أكثر من ذلك فيمكنك تحديد الوقت أو عدد الثوانى التى يتم طرده بعدها وذلك كله يتم من خلال عدة معاملات يمكن إضافتها إلى الأمر shutdown كل معامل منها عند إضافته للأمر يكون مسئول عن تنفيذ أمر معين والجدول التالى يوضح ذلك كله .

وظيفة الأمر	صيغة الأمر	المعامل
يقوم هذا الأمر بعمل Restart (إعادة تشغيل للجهاز)	Shutdown -r	-R
يقوم هذا الأمر بإجبار جميع البرامج المفتوحة على الإغلاق وعمل خروج للمستخدم دون إظهار رسائل	Shutdown –f	-F
يقوم هذا الأمر بعمل خروج للمستخدم بعد عدد الثوانى التى تحددها بنفسك والمعامل X يرمز إلى عدد الثوانى فمثلاً الأمر shutdown –t 15 يقوم بعمل خروج للمستخدم بعد 15 ثانية ودون ظهور رسائل	Shutdown –t x	-T x

يمكنك إختيار الأمر المناسب لك من الجدول السابق وكتابته داخل البرنامج الدفعى بدلاً من الأمر Shutdown –s الذى أدخلناه من قبل .



الفصل الحادي عشر

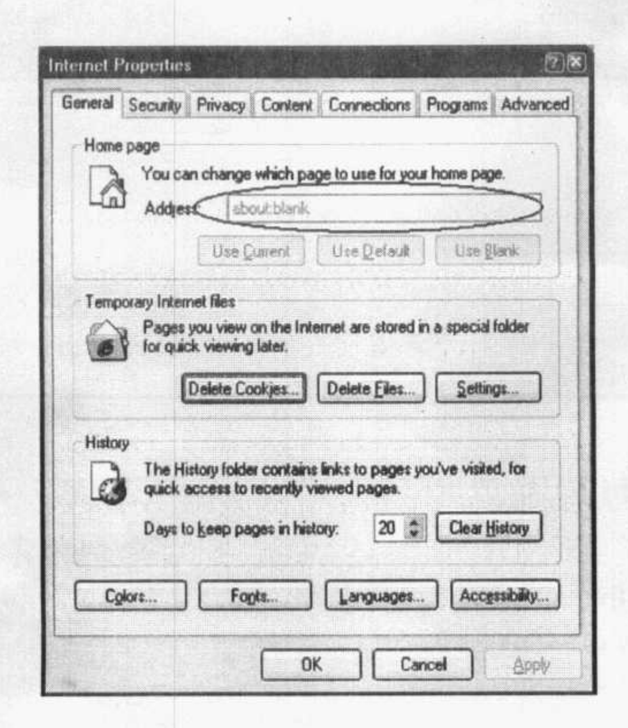
مخاطر الإنترنت والشبكات

مخاطر الإنترنت والشبكات

أعتقد أنك الأن بعد كل ما تعرضنا له وتعلمته فـي الفـصول السابقة أصبحت لديك المقدرة على مواجهة وتحدى أى شخص تسول له نفسه العبث بجهاز أثناء غيابك .. ولكن عند الحديث عن الإنترنـت أو الشبكات ستجد أن الموقف قد إختلف لما لهذا الجانب من تشعبات وأبعاد أخرى يجب وضعها فى الحسبان لذلك سنتحدث فى هذا الفـصل عـن بعض الأشياء الهامة التى يمكن أن نتعرض لها خـلال عملنـا علـى الإنترنت وكيف يمكن لنا تجنبها .. فعلى سبيل المثال فإن من الأشـياء الشائعة أن بعض المواقع تقوم بفرض نفسها علـى الـصفحة الأولـى للمتصفح وتمنع المستخدم من محاولة تغيير أو تعديل ذلك وتجد نفـسك فى كل مرة تتدخل فيها على الانترنت لا بد من الدخول على هذا الموقع أولاً بما يشبه عملية إختطاف ! أيضاً سنتعرض لخاصية التشارك عبـر الشبكات وكيف نستطيع أن نقوم بتأمين هذا التشارك بأكثر من شكل وما إلى ذلك مما يسمح لنا بتفادى الكثير من المشاكل التى يمكن أن تحـدث لنا أثناء الإبحار فى عالم الانترنت .

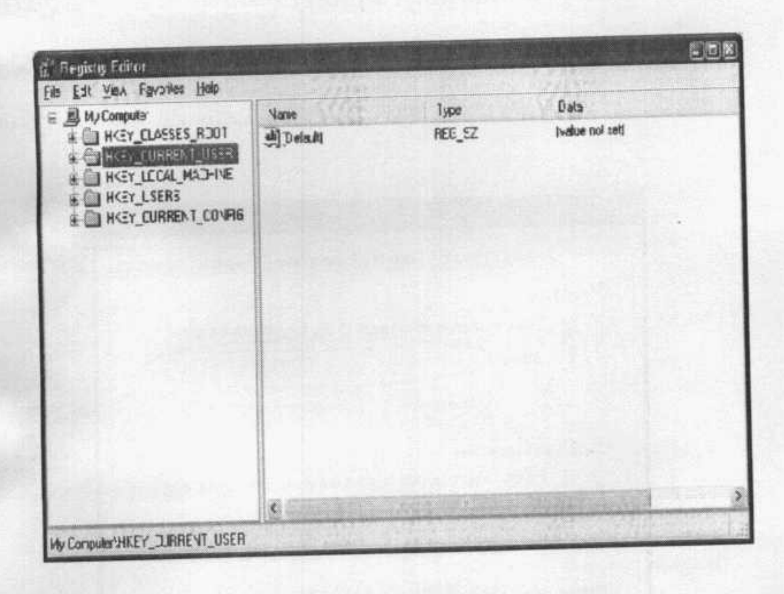
استعادة صفحة البداية للمتصفح :

ظهرت فى الآونة الأخيرة بعض المواقع التى تفـرض نفـسها على صفحة البدء لمتصفح الانترنت وعند محاولة تعديل ذلك من خلال نافذة خصائص الإنترنت والتى تظهر لك عن طريق نقر زر المـاوس الأيمن فوق أيكونة المتصفح Internet Explorer فوق سطح المكتـب وإختيار properties من القائمة المختصرة ستجد أن تعديل ذلك غيـر ممكن وستظهر لك النافذة كما بالشكل التالى :



كما ترى فقد تم إغلاق الخاصية لمنع المستخدم من التعديل فيها ولحل هذه المشكلة وإعادة هذه الخاصية إلى العمل اتبع الخطوات التالية :

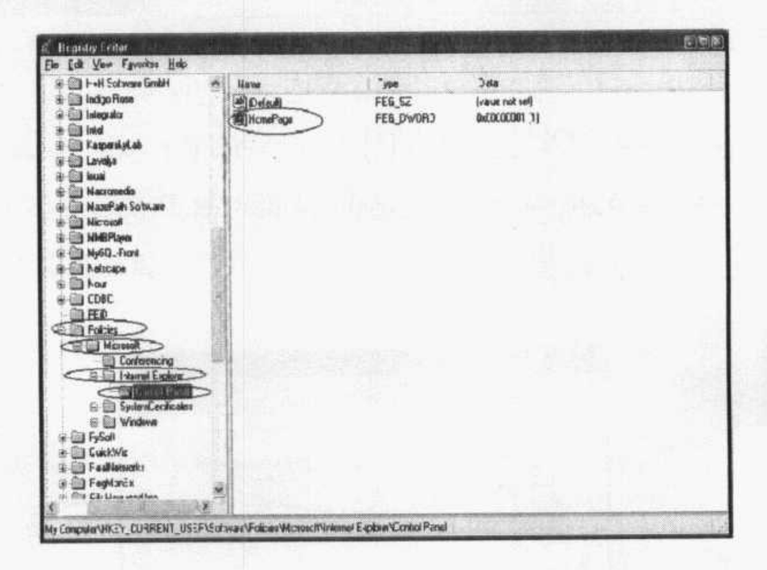
قم بفتح صندوق Run من قائمة start ثم أكتب داخله الأمر regedit ثم اضغط Enter لتفتح لك نافذة محرر السجل كما بالشكل التالى :



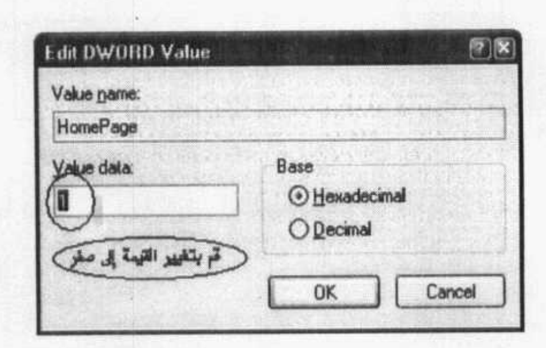
من النافذة السابقة ومن تحت HKEY_CURRENT_USER قم بالذهاب إلى المسار التالى

Software \ Policies \ Microsoft \ Internet Explorer \ Control Panel

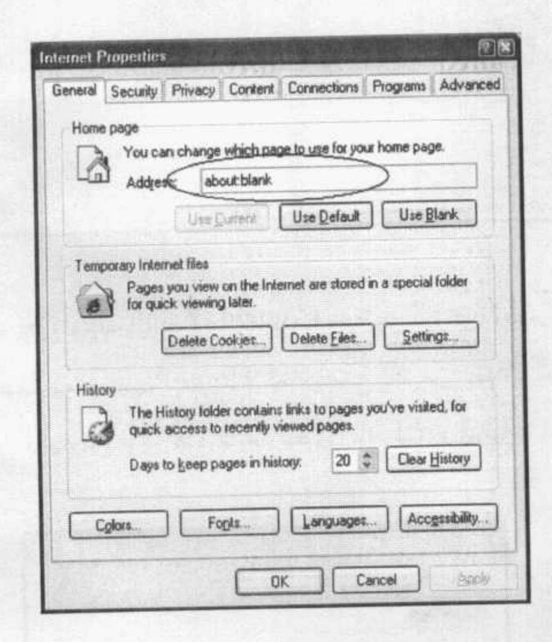
لتصبح النافذة كما يلى :



بعد الوقوف على مجلد Control Panel سيظهر لك فى الجانب الأيمن من النافذة قيمة بإسم HomePage كما يتضح لك من الشكل السابق قم بالنقر مرتين بالماوس فوق هذه القيمة لتظهر لك النافذة التالية :

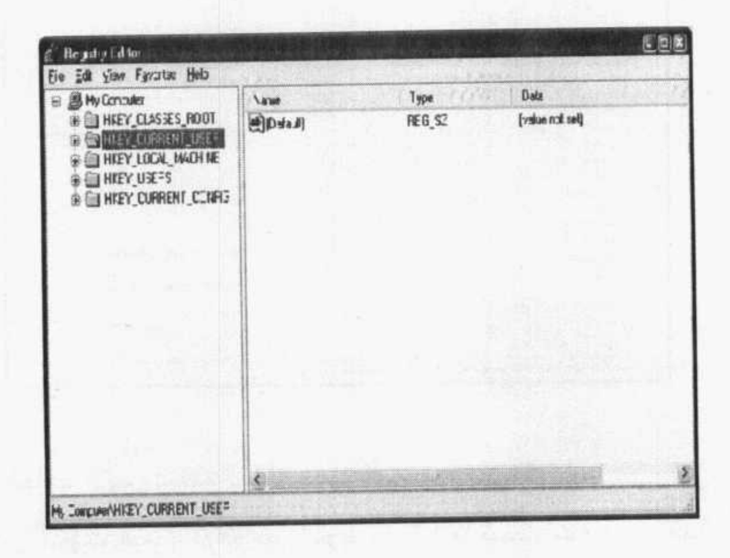


من النافذة السابقة وفى صندوق النص أسفل Value data قـم بتغييـر القيمة إلى صفر (0) بدلاً من واحد (1) ثم أنقر زر Ok ثم قـم بفـتح نافذة internet Properties مرة أخرى وستجدها هذه المرة أصـبحت كما بالشكل التالى :



يمكنك أيضاً تغيير صفحة البدء للمتصفح بطريقة أخرى عـن طريـق كتابته بنفسك من خلال محرر السجل وذلك بفتح صـندوق Run مـن

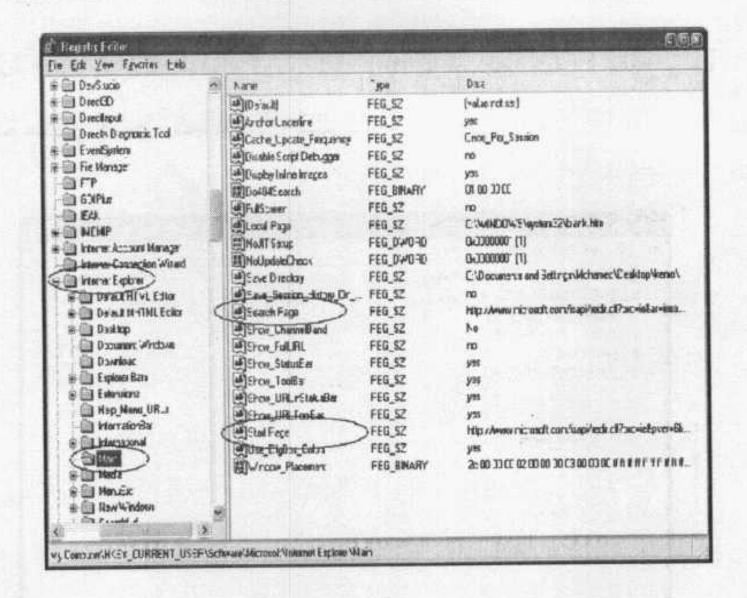
قائمة start ثم أكتب داخله الأمر regedit ثم اضغط Enter لتفتح لـــك نافذة محرر السجل كما بالشكل التالى:



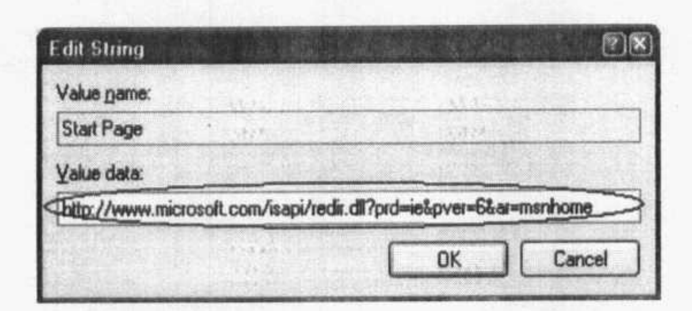
من النافذة السابقة ومن تحـــت HKEY_CURRENT_USER قـــم بالذهاب إلى المسار التالى ..

Software \ Microsoft \ Internet Explorer \ Main

لتصبح النافذة كما يلى :

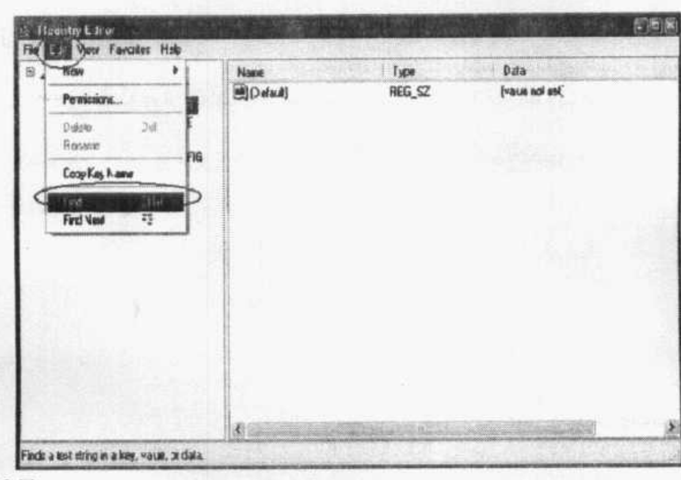


فى الجانب الأيمن للنافذة السابقة ستجد قيمة باسم Search Page والتى تخص محرك البحث الإفتراضى للويندوز أما ما تبحث عنه فهى القيمة Start Page الخاصة بصفحة البداية للمتصفح فقم بالنقر مرتين فوقهـا لتظهر لك هذه النافذة .

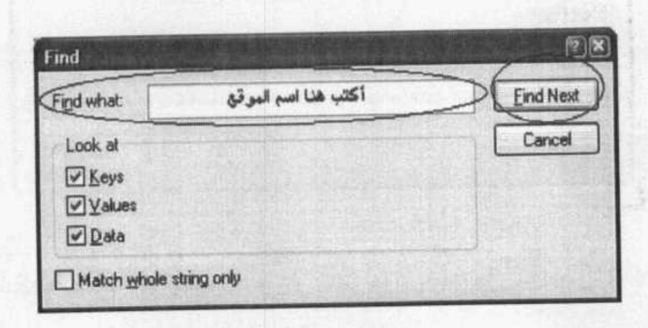


من النافذة السابقة قم بحذف العنوان الموجود بصندوق الـنص وأكتب عنوان الموقع الذى تريده ثم انقر الزر OK .

يمكنك أيضاً التخلص من الموقع الذى يقوم بفرض نفسه عليك بطريقة أخرى من خلال محرر السجل عن طريق فتح قائمة Edit وإختيار الأمر Find كما يلى :



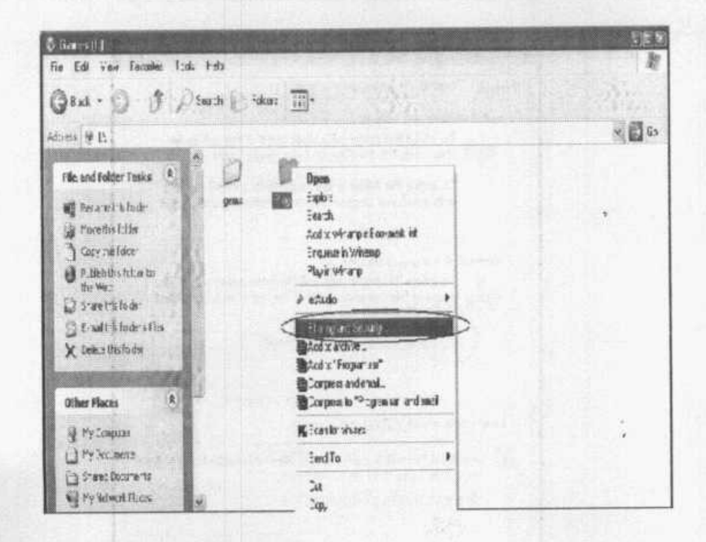
لتظهر لك نافذة البحث التالية :



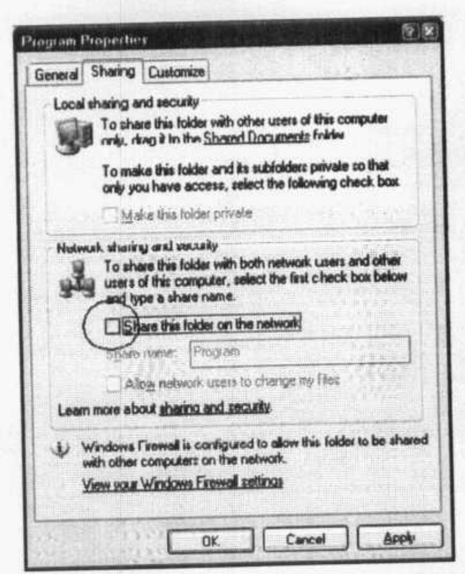
قم بكتابة اسم الموقع فى صندوق النص أمام Find what ثم انقر الزر Find Next ليبدأ البحث داخل ملفات النظام عن الأوامر التى بها هـذا الموقع وعندما تجدها قم بحذفها .

التشارك بالمجلدات :

فى الطريقة العادية عندما تريد مشاركة أحد المجلدات تقوم بنقر زر الماوس الأيمن فوق هذا المجلد لتظهر قائمة مختصرة كما بالشكل التالى :

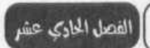


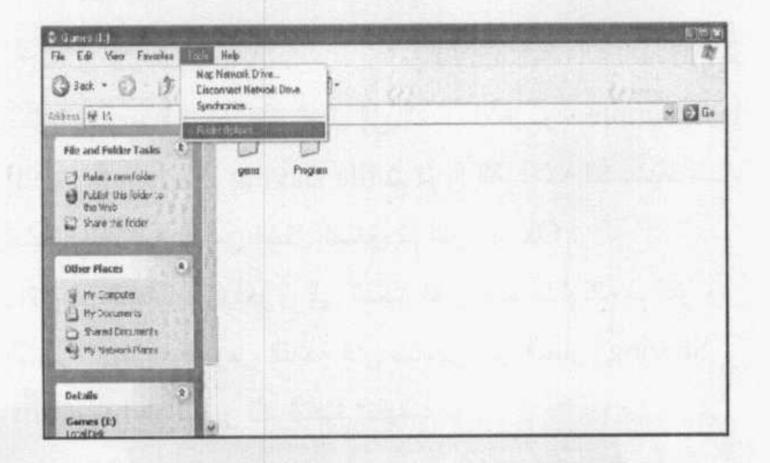
ومن القائمة التى تظهر تقوم بنقر الخيار Sharing and Security لتظهر لك النافذة التالية :



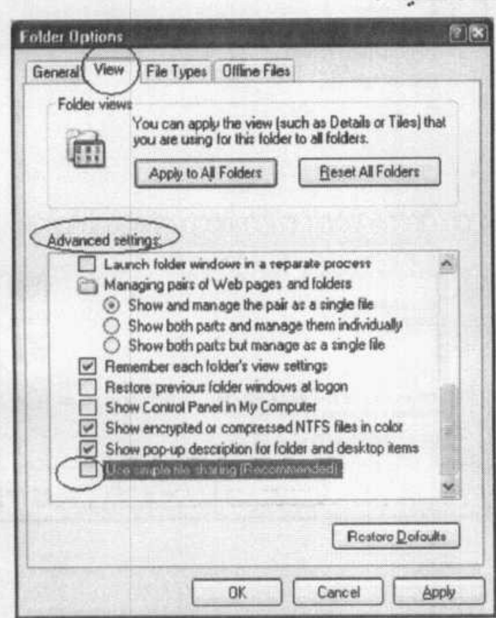
ومن النافذة السابقة تقوم بتنشيط الخيـــار Share this folder on the network الوضح لك بالشكل السابق ... ولكننا هنا نريـــد أن نفـــرض بعض القيود لحماية هذا المجلد وتأمينه كأن تسمح لعـــدد معـــين مـــن الأشخاص بالتعامل مع هذا المجلد وتحديد مدى صلاحية كل منهم فـــى التعامل معه وهكذا ولكننا لا يمكنا ذلك من خلال النافذة السابقة والتـــى يظهر لنا من خلالها نظام المـــشاركة المبـــسط الـــذى هـــو الوضـــع الإفتراضى لإعدادات الويندوز ولكى نقوم بإستخدام الطريقـــة المتقدمـــة والتى تتيح لنا تطبيق ما نريده علينـــا أولاً أن نقـــوم بإيقـــاف خاصـــية المشاركة البسيطة هذه وللقيام بذلك عيك إتباع الخطوات التالية .

من قائمة Tools قم بإختيار Folder Options كما يلى :



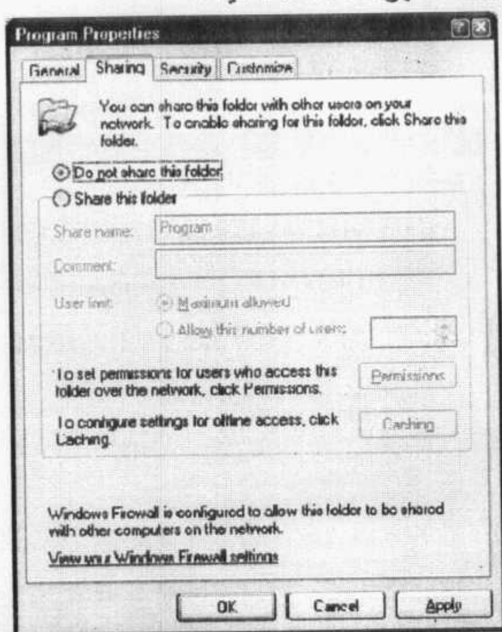


لتظهر لك النافذة التالية :

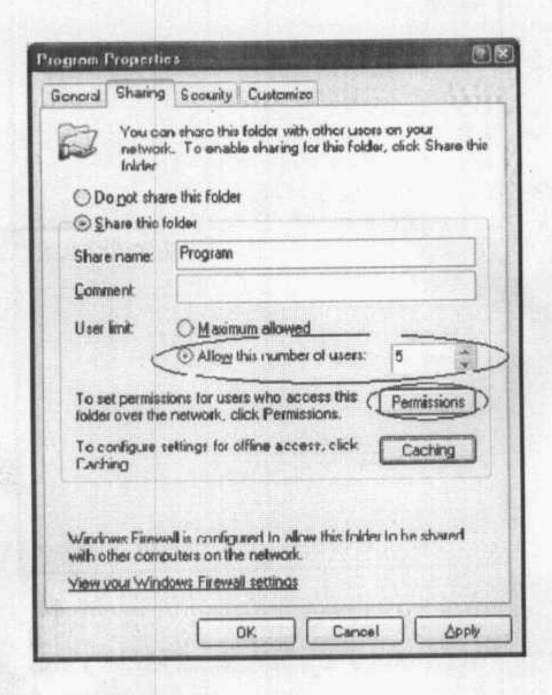


من خلال التبويب View ومن تحت الجزء Advanced settings قم بتحريك شريط التمرير حتى تصل إلى الخيار الأخيــر Use simple file sharing [Recommended] ثم قم بإزالة علامة التنــشيط مــن أمامه كما يتضح لك من الشكل السابق ثم انقر زر Ok .

والأن قم بالذهاب مرة أخرى إلى المجلد الذى تريد مشاركته ثم انقر زر الماوس الأيمن فوقه ومن القائمة التى ستظهر انقر الخيار Sharing and Security لتظهر لك النافذة التالية :

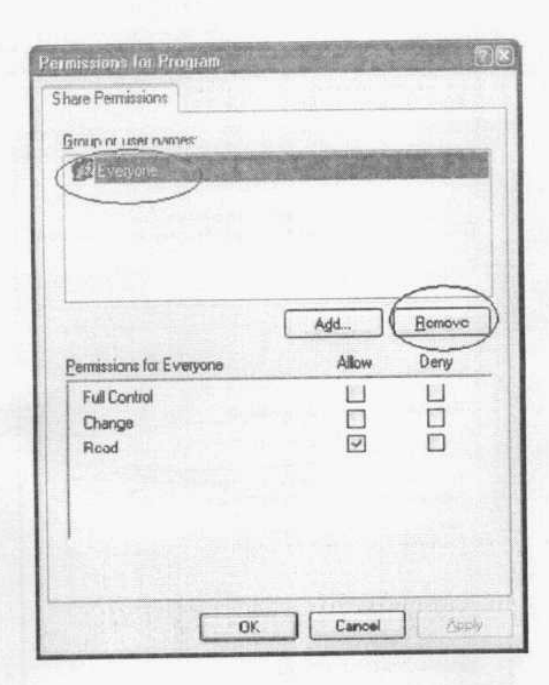


لاحظ فى هذه المرة تغير محتويات النافذة عن المرة الـــسابقة ولتفعيـــل مشاركة المجلد قم بتنشيط الخيار Share this folder لتتاح لك بـــاقى الخيارات كما يلى .

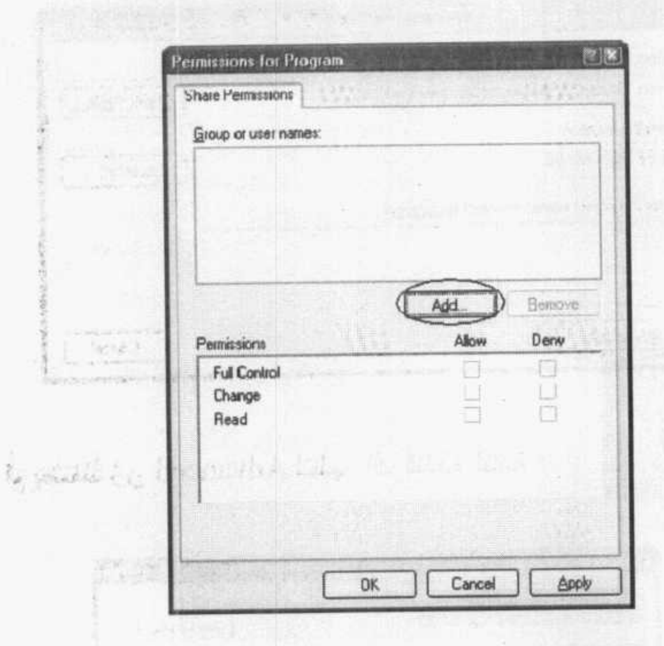


فى الجزء الخاص الخاص User limit قم بتنـــشيط الخيـــار Allow this number of users ثم قم بتحديد عدد المستخدمين الذين تريد لهم

إستخدام هذا المجلد كما يتضح ثم انقر الزر Permissions لتظهر لـــك النافذة التالية :

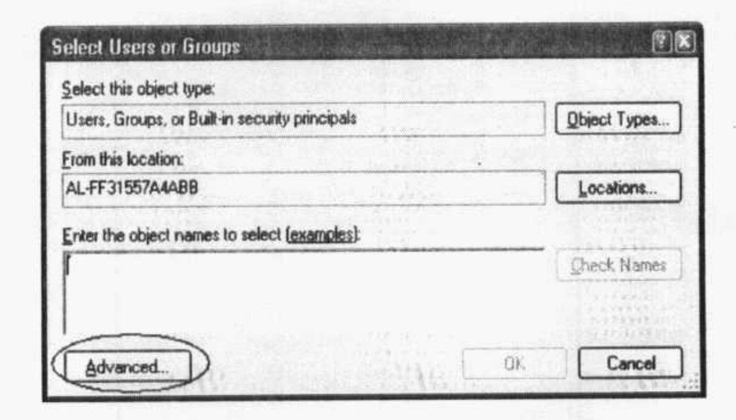


يظهر لك فى النافذة السابقة أســفل الجــزء Group or user names كلمة Everyone أى أن كل الموجودين على الشبكة سيتاح له الوصول إلى هذا المجلد فقم بضغط زر Remove لحذف هذا الإختيار وتــصبح النافذة خالية كما يلى :

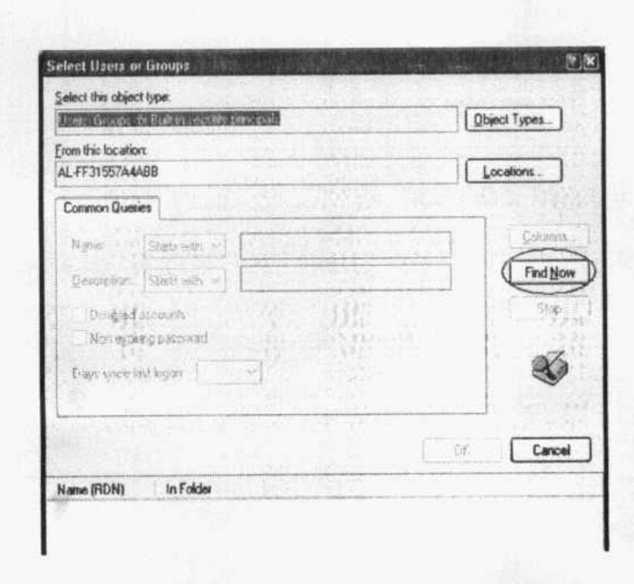


قم الأن بنقر زر Add لإضافة الأشخاص أو المجموعات الذين تريد أن يتعاملوا مع المجلد لتظهر لك النافذة التالية :

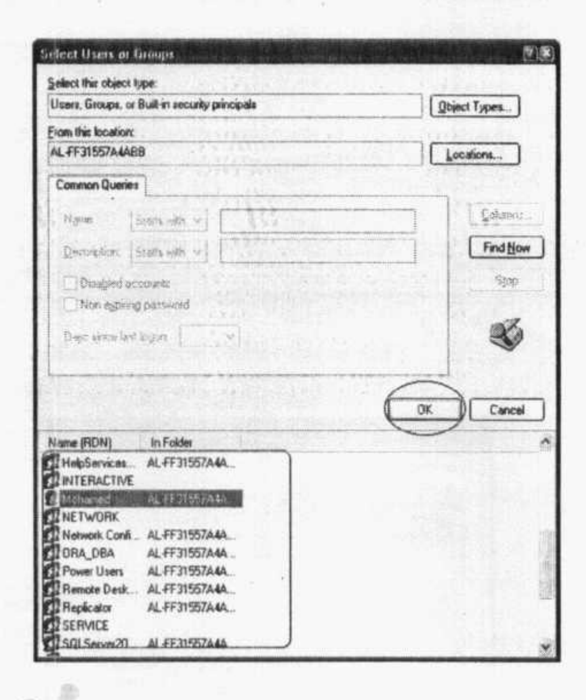




قم بضغط زر Advanced لتظهر لك النافذة التالية :

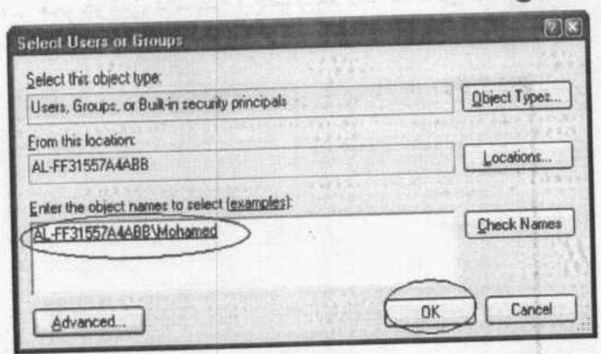


قم بنقر الــزر Find Now ليــتم البحــث عــن أســماء الأشــخاص والمجموعات الموجودين بالشبكة وإظهارهم كما بالشكل التالى :



يظهر لك أسفل النافــذة الــسابقة أســماء المجموعــات والمــستخدمين الموجودين بالشبكة فقم بإختيار ما تريده من مجموعات أو مــستخدمين وكمثال هنا سنختار اسم المستخدم Mohamed ثــم أنقــر الــزر Ok

لتختفى النافذة وتعود ألى النافذة السابقة لها وقد اضـــيف الأســـم الـــذى أخترته كما يلى :



قم بنقر زر Ok لتعود إلى هذه النافذة :

Permissions for Program
Share Permissions
Group or user names:
Mohamed (AL-FF31557A4ABB\Mohamed)
Add...
Remove
Permissions for Mohamed
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply

تظهر النافذة السابقة أسماء المستخدمين الذين متاح لهم الوصــول إلــى المجلد وكما ترى يوجد مستخدم واحد فقط هو ما قمنا بالسماح له بــذلك ويوجد أسفل الجــزء Permissions for Mohamed الــصلاحيات المتاحة لهذا المستخدم ويوجد ثلاث إختيارات هى :

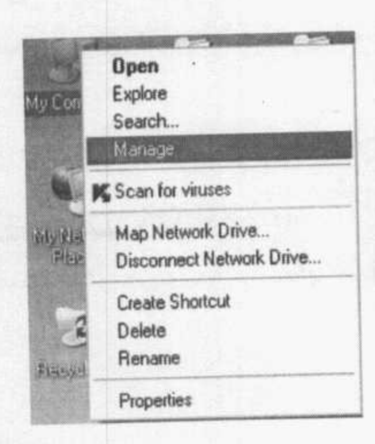
- **Full Control** : أى تحكم كامل بالمجلد .
- **Change** : يسمح للمستخدم بالحصول على معظم الصلاحيات السابقة غير أنه لا يمكنه تغيير صلاحية الوصول إلى المجلد أو الحصول على ملكيته .
- **Read** : يسمح له بحق القراءة فقــط دون التعــديل علـــى أى شيء .

بعد أن تنتهى من أضافة وإختيار ما تريد قم بنقر الزر OK لتعود إلــى النافذة الأولى فقم أيضاً بنقر زر OK الخاص بها .

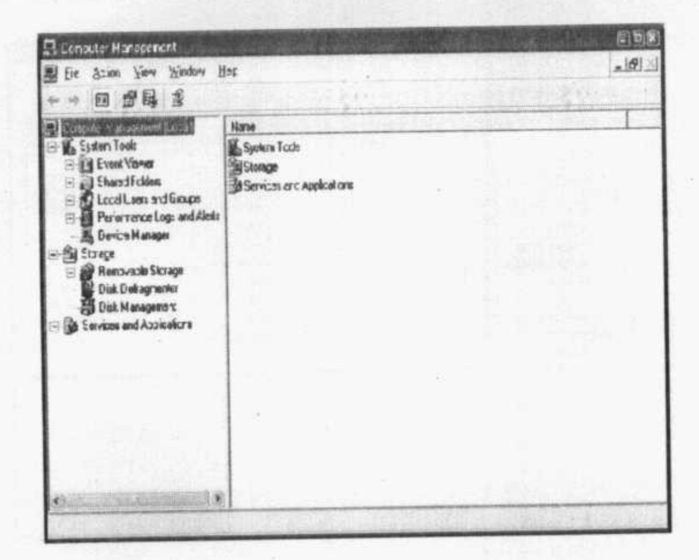
لاحظ أنه يمكنك إضافة أكثر من مستخدم وتحديد صلاحيات مختلفــة لكل منهم على حدى .

المشاركات الخفية :

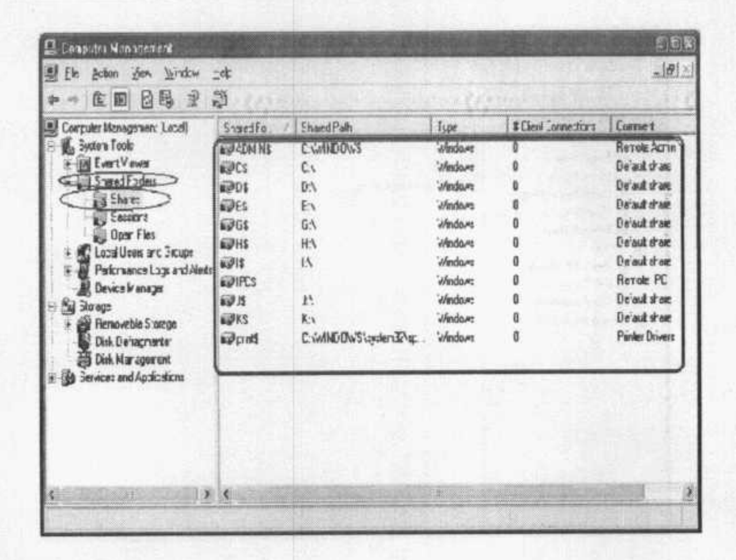
يعتقد الكثير أن الأقراص أو المجلدات المتشاركة على الجهاز هى التى يقوم المستخدم بتفعيل خاصية التشارك لها وهذا إعتقاد خاطىء ... لأنه توجد مجلدات يقوم الويندوز بالتشارك بها تلقائياً بغرض الإشراف (من قبل مشرفى الشبكات) ولمعرفة الأجزاء المتشارك بها قم بالذهاب إلى سطح المكتب ثم انقر زر الماوس الأيمن فوق رمز My Computer لتظهر لك قائمة مختصرة كما بالشكل التالى:



من القائمة التى ظهرت لك قم بنقر الخيار Manage لتظهر النافذة التالية :



من الجانب الأيسر للنافذة السابقة قم بنقر علامـــة (+) بجـــوار مجلد Shared Folders ليتفرع منه عدة مجلدات أخر قم بالنقر منهـا على المجلد Shares كما بالشكل التالى :



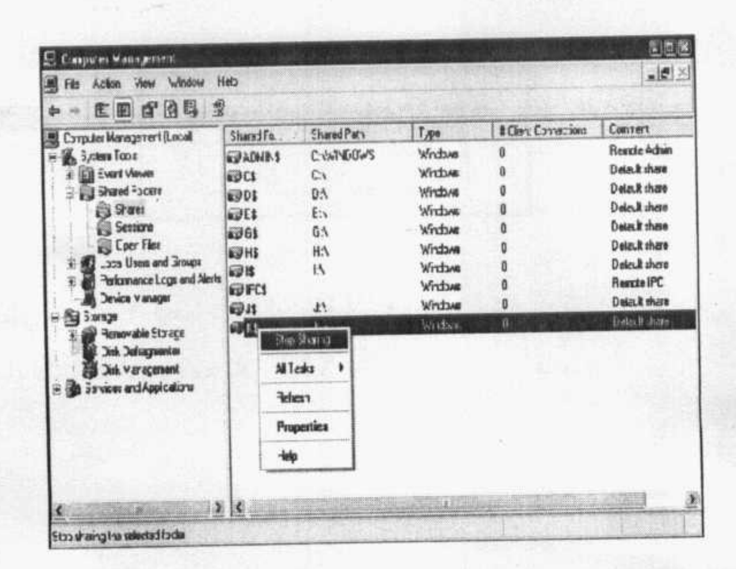
يظهر لك فى الجانب الأيمن من النافذة الـسابقة الأجـزاء التـى قـام الويندوز بالتشارك بها تلقائياً وهذه الأجزاء عبارة مجلد ملفات الويندوز و الأقراص الموجودة على الحاسب بالإضافة إلى Ipc وهو يرمز إلـى جزء من الذاكرة يستخدم فى إستعراض المصادر المتشارك بهـا علـى حاسب أخر كما يستخدم عند الإشراف على الحاسب من بعد أما الأسـم التشاركى Print فهو يرمزإلى المجلد الموجود به مشغل الطابعة وقـد أتاحه ويندوز أيضاً للتشارك من أجل أن تتمكن باقى الحاسبات من نسخ هذا المشغل فى حالة وجود طابعة متشارك بها على الشبكة **لاحظ** أيضاً

وجود علامة الدولار ($) بجوار الأجزاء المتشارك بها دليل علـــى أن هذه المشاركة مخفية .

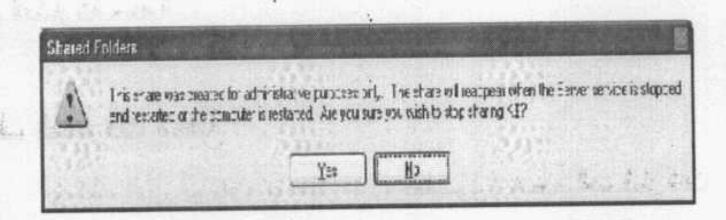
إيقاف المشاركات الخفية :

يمكنك الأن أن تقوم بتحديد مدى خطـــورة هـــذه المـــشاركات المخفية .. أو فائدتها إن كان جهازك يخضع للعمل داخل شبكة أمـــا إذا أردت إيقاف هذه التشاركات فإليك الطريقة .

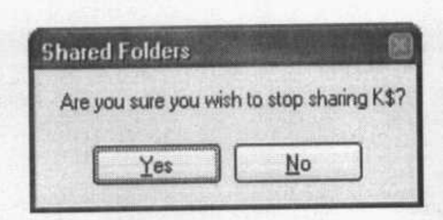
قم بنقر زر الماوس الأيمن فوق الرمز الذى تريد إيقاف لتظهر لك قائمة مختصر كما يلى :



قم باختيار Stop Sharing من تلك القئمة لتظهر لك الرسالة التالية :



تخبرك الرسالة السابقة بعودة هذا التشارك وهذه الخدمة من جديد عند تشغيل الجهاز فى المرة القادمة قم بنقر زر Yes لتظهر لك الرسالة التالية :

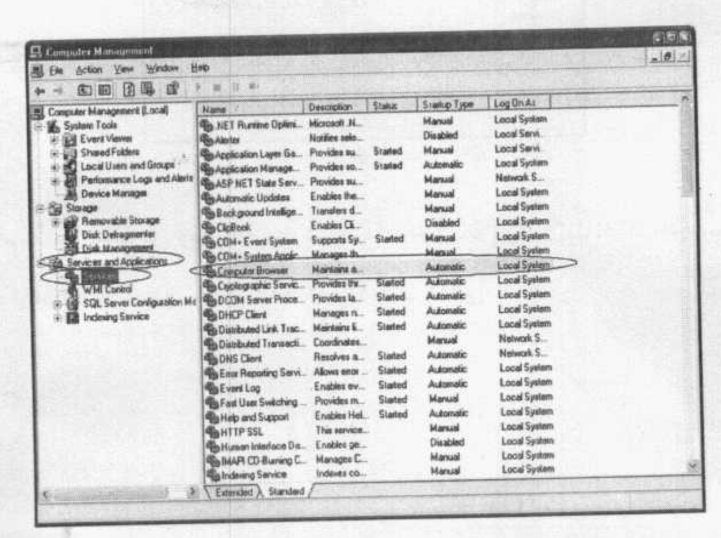


قم بنقر زر Yes أيضاً لهذه الرسالة لأيقاف ذلك التشارك ثم كرر هذه الخطوات مرة أخرى مع باقى الأجزاء المتشارك بها لإيقافها ...

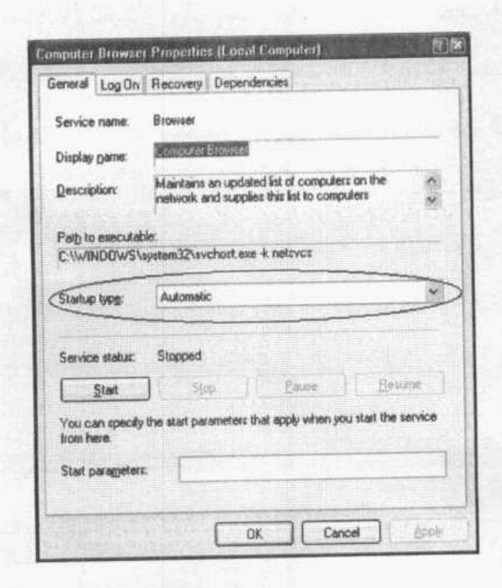
إيقاف خدمة التشارك :

كما لاحظت وبينت لك الرسالة فى الخطوات الـسابقة أن هـذا التشارك سيعود للعمل مرة أخرى فى المرة القادمة لتشغيل الويندوز أو عند عمل Restart للجهاز وفى هذه الحالة عليك أن تعيد هذه الخطوات مرة أخرى ... لذلك فإنك إذا أردت إيقاف هذه الخدمة بحيث لا تعـود مرة أخرى للعمل عند إعادة تشغيل الجهاز فتابع الخطوات التالية :

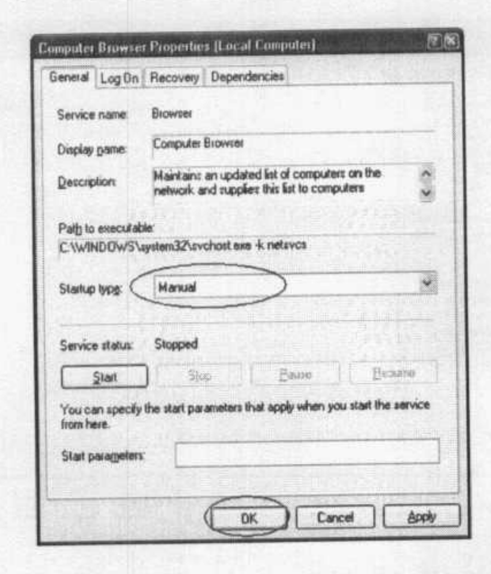
قم بفتح نافذة Computer Management كما تعلمت من قبل ثم فـى الجانب الأيسر منها قم بالضغط على علامـة (+) بجـوار Services and Applications لتتفرع منها عدة تفريعات أخرى قـم بـالوقوف منها على Services لتصبح النافذة كما بالشكل التالى :



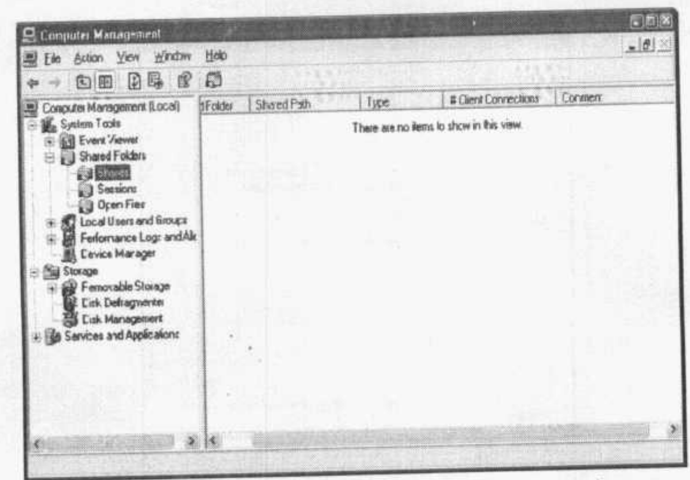
فى الجانب الأيمن من النافذة قـم بالبحـث عـن البنـد Computer Browser والموضح لك بالشكل السابق ثم انقر فوقه بالماوس مـرتين لتظهر لك النافذة التالية :



قم بالنقر بالماوس فوق القائمة المنسدلة بجوار Startup type لفتحهـا واختار منها الخيار Manual كما بالشكل التالى :



ثم انقر الزر Ok وأعد تشغيل الجهاز وعند محاولـــة رؤيـــة الملفـــات المتشارك بها ستجدها كما يلى:

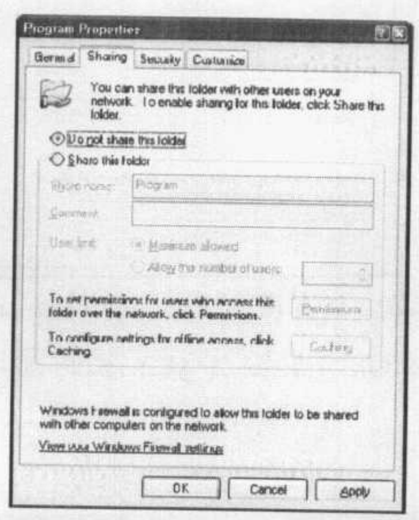


ولكن لاحظ أنك بذلك ستفقد أى تشارك قمت به مسبقاً لأى مجلد كما أنك لن تتمكن من عمل أى تشارك أخر أثناء توقف هذه الخدمة .

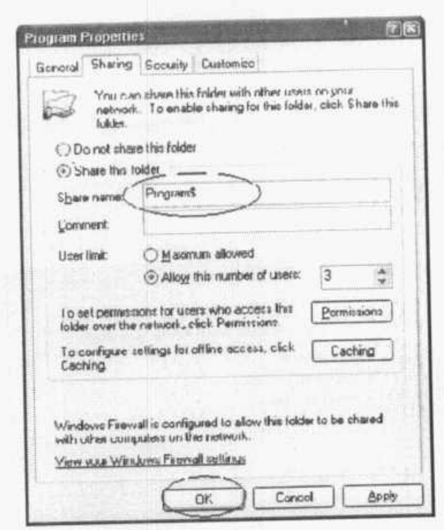
إخفاء التشارك :

يمكنا نحن أيضاً أن نستفيد من هذه الميزة ! ونقوم بإخفاء المجلدات أو العناصر التى نريد مشاركتها على الشبكة بحيث أنه حين يقوم أحد المستخدمين بإستعراض المجلدات المتشارك بها من خلال My Network Places فإنه لا تظهر له هذه المجلدات أو يعلم بها وهذه الطريقة جيداً جداً لحماية الملفات فى حالة إقتحام الشبكة من أحد الغرباء ولكن لاحظ أنه بد من إعادة خدمة التشارك التى قمنا بإيقافها من قبل إلى العمل ثم تابع الخطوات التالية :

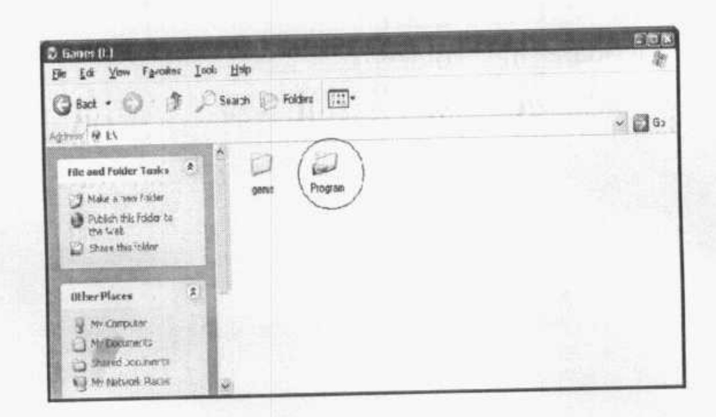
كالعادة قم بالذهاب إلى المجلد الذى تريد مشاركته ثم انقر زر الماوس الأيمن فوقه ومن القائمة التى ستظهر انقر الخيار Sharing and Security لتظهر لك النافذة التالية :



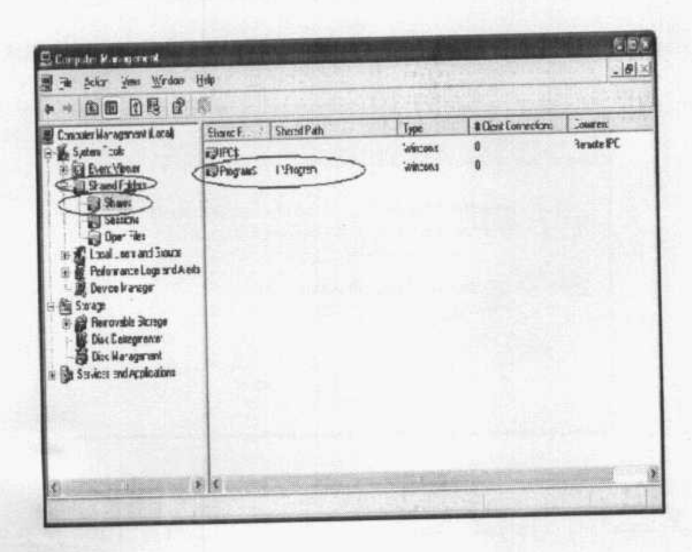
لتفعيل مشاركة المجلد قم بتنشيط الخيار Share this folder لتتاح لك باقى الخيارات كما يلى :



كل ما سنقوم به هو إضافة رمز الدولار ($) إلى اسم المشاركة الخاص بالمجلد كما يتضح لك بالشكل السابق ثم انقر الزر Ok ليصبح المجلـد كما بالشكل التالى .



كما ترى المجلد يظهر بالشكل العادى ولكن عند إستعراض المجلدات المتشارك بها من خلال نافذة My Network Places فلن يظهر هذا المجلد ولكن إذا قمت بالذهاب إلى نافذة Computer Management ستجد المجلد موجود وبجواره رمز الدولار كما يلى :

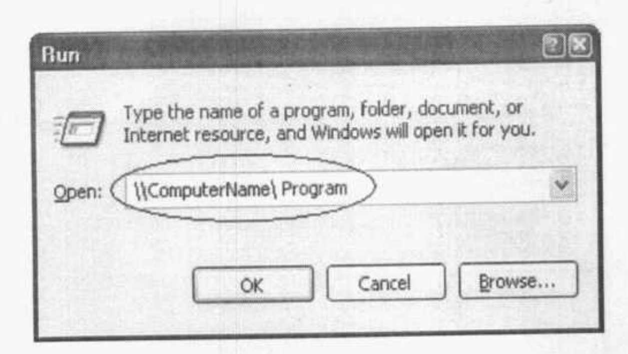


كيفية الوصول إلى المجلد :

ولعلك تسأل بما أن المجلد لن يظهر على الشبكة وبالتالى لن يستطيع أحد رؤيته فكيف إذاً سنتمكن من التعامل معه أو الإستفادة منه ؟! ولكن قبل أن أجيبك فعليك أن تعرف أن تلك الحيرة أو هذا اللغز

الذى تسأل عنه هو فى الحقيقة الميزة التى قمنا من أجلها بإستخدام التشارك الخفى لأنه لن يستطيع أحد التعامل مع هذا المجلد إلا الأشخاص الذين تخبرهم أنت بوجود المجلد وتريدهم أن يتمكنوا من الوصول إليه وذلك عن طريق الخطوات التالية .

إذا كنت تريد التعامل مع أحد التشاركات المخفية على أحد أجهزة الشبكة قم بفتح صندوق Run من قائمة start ثم أكتب داخله **\\ComputerName\ Program** كما بالشكل التالى :



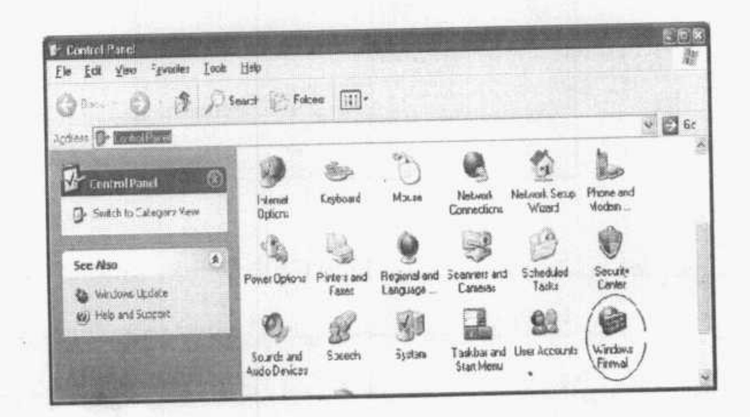
حيث يرمز ComputerName إلى اسم الجهاز الموجود به المجلد أما Program فهو اسم المشاركة الخاص بالمجلد .

لاحظ أنه يمكنك الإستفادة من هذه الميزة فى أشياء أخرى مثل مشاركة الطابعات .

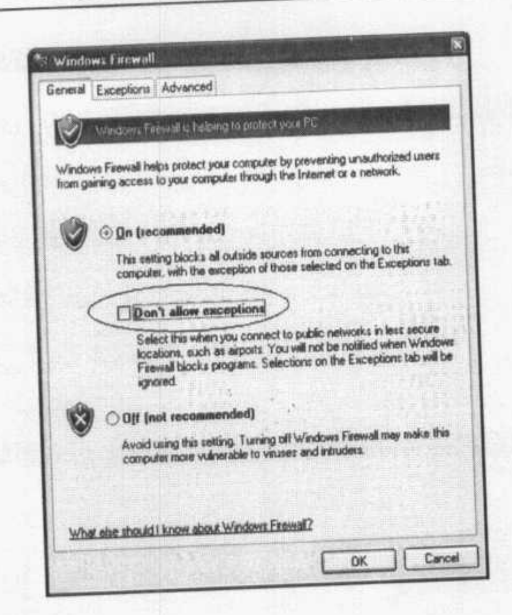
التحكم فى الحائط النارى :

يحتوى ويندوز XP على برنامج Firewall وهـذا البرنـامج مسئول عن مراقبة حركة دخول البيانات وخروجها على الحاسب ويقوم بمنع أى محاولة غير مشروعة يمكن أن تتم لنقل أو ارسـال البيانـات ويمكنك التحكم فى عمل هذا الحائط النارى كما يلى .

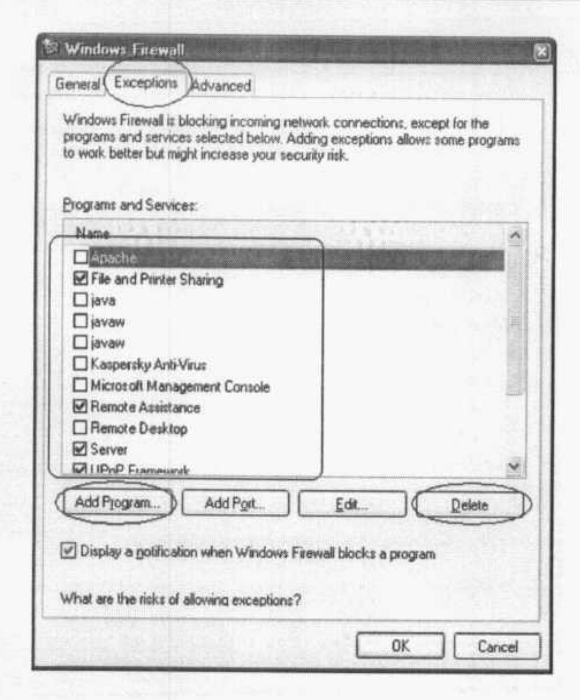
قم بالدخول إلى لوحة التحكم Control Panel كما يلى :



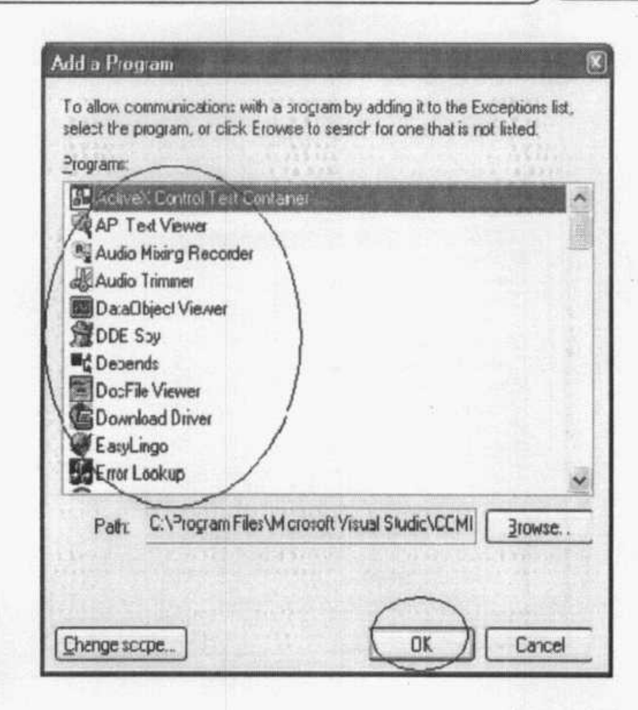
قم بالنقر مرتين فوق أيكونة Windows Firwall لتفتح لـك النافـذة التالية :



الخيار Don't allow exceptions يتيح لك مستوى تأمين أعلى حيث سيتم منع أى محاولة دخول على الحاسب حتى وإن كانت من خلال البرامج المسموح لها بذلك ولمعاينة البرامج والخدمات التى يسمح لها بالإتصال بالحاسب قم بنقر التبويب Exceptions كما يلى :



كما موضح لك بالشكل السابق يمكنك إزالة التنشيط من أمام البرنـــامج الذى لا تريد السماح له الإتصال بالحاســـب أو أن تنقـــر زر Delete لحذفها من القائمة كما يمكنك التأشير أمام البرامج التى تريد السماح لها بذلك وإذا لم يكن البرنامج الذى تريده فى هذه القائمة يمكنـــك أن تنقـــر الزر Add program لتفتح لك النافذة التالية :



من النافذة السابقة يمكنك إختيار البرنامج الذى تريده ثم انقر Ok ليــتم إضافته إلى قائمة البرامج المصرح لها بالإتصال بالحاسب .

الفهرس

الفصل الأول

إغلاق الأبواب

إغلاق الأبواب 8

إنشاء كلمة سر : 9

حل أخر لنسيان كلمة المرور : 14

الفصل الثاني

الأبواب الخلفية

الأبواب الخلفية 26

كيف يتم إختراق الويندوز من خلال ال Administrator ؟؟ 27

إظهار حساب Administrator دائماً في شاشة الدخول للويندوز : ... 30

إخفاء Administrator من شاشة الدخول إلى الويندوز في كل الأحوال ! :
.... 34

حساب الضيف Guest : 39

تشغيل حساب Guest : 40

وضع كلمة مرور لحساب Guest : 43

حذف كلمة مرور حساب Guest : 45

حذف كلمة المرور : 50

الفصل الثالث

مزيد من الأمان

مزيد من الأمان 52

إخفاء مستخدم من شاشة دخول الويندوز : 52

جعل كلمات المرور أكثر فاعلية : 55

تحديد عدد حروف كلمات السر : 59

تحديد الحد الأقصى لفترة كلمات السر : 60

تحديد مستوى التعقيد فى كلمات السر : 61

الفصل الرابع

مفتاح إقلاع للويندوز

مفتاح إقلاع للويندوز 68

برامج حذف كلمات المرور : 69

إنشاء قرص لإقلاع الويندوز : 79

الفصل الخامس

مراقبة الويندوز وتسجيل محاولات الإختراق !

مراقبة الويندوز وتسجيل محاولات الإختراق ! 86

تشغيل برنامج Event Viewer : 88

تفعيل خاصية مراقبة التهديدات الأمنية : 89

الفصل السادس

إزالة الآثار

إزالة الآثار 102

حذف محتويات قائمة المستندات الأخيرة : 103

حذف قائمة المستندات الأخيرة عند الخروج : 115

حذف محتويات مجلد prefetch : 118

منع تتبع المستخدم : 120

الفصل السابع

حماية الأقراص

حماية الأقراص 128

إخفاء محركات الأقراص : 128

منع الوصول إلى الأقراص : 141

إخفاء عناصر سطح المكتب : 143

الفصل الثامن

حماية الملفات

حماية الملفات 150
تشفير الملفات : 150
إخفاء إمتداد الملفات : 155

الفصل التاسع

منع التحكم بنظام التشغيل

منع التحكم بنظام التشغيل 164
منع الوصول إلى لوحة التحكم Control panel : 164
إزالة البرامج من قائمة start : 171

الفصل العاشر

ويندوز اكس بى يطرد الغرباء !

ويندوز اكس بى يطرد الغرباء ! 178
إنشاء الملف الدفعى : 179

الفصل الحادي عشر

مخاطر الإنترنت والشبكات

مخاطر الإنترنت والشبكات 200
استعادة صفحة البداية للمتصفح : 201
التشارك بالمجلدات : 208
المشاركات الخفية : 220
كيفية الوصول إلى المجلد : 231
التحكم فى الحائط النارى : 233

رقم الإيداع
25139 / 2007



المركز الرئيسي : 11 شارع د/محمد رأفت – محطة الرمل – الإسكندرية
تليفون وفاكس : 4838326 (03)(2+)
موبايل : 0101634294 (2+) - 0123357844 (2+)
Email: info@egyptbooks.net
URL: www.egyptbooks.net